Indian Statistical Institute Kolkata Tech. Rep. no. ASD/2010/3, November 10, 2010
Revised draft August 1, 2011

Key Predistribution Schemes for Distributed Sensor Networks via Block Designs

Mausumi Bose[a 1], Aloke Dey[b], Rahul Mukerjee[c]

[a] *Indian Statistical Institute, Kolkata 700108, India*

[b] *Indian Statistical Institute, New Delhi 110016, India*

[c] *Indian Institute of Management Calcutta, Kolkata 700104, India*

Abstract Key predistribution schemes for distributed sensor networks have received significant attention in the recent literature. In this paper we propose a new construction method for these schemes based on combinations of duals of standard block designs. Our method is a broad spectrum one which works for any intersection threshold. By varying the initial designs, we can generate various schemes and this makes the method quite flexible. We also obtain explicit algebraic expressions for the metrics for local connectivity and resiliency. These schemes are quite efficient with regard to connectivity and resiliency and at the same time they allow a straightforward shared-key discovery.

1 Introduction

Distributed sensor networks have been extensively studied in recent years due to their wide applicability in both civilian and military contexts. For instance, in a military operation, sensor nodes may be distributed in a random manner over a sensitive area and, once deployed, these nodes are required to communicate with each other in order to gather and relay information. This communication has to be done in a secret manner and so secure keys need to be established between the nodes in the system. For more details on the applications, the security framework and models for these distributed sensor networks (DSNs) we refer e.g., to Carmen et al. (2000), Roman et al. (2005) and Du et al. (2005). There are also interesting results pertaining to an

[1] Corresponding author.

email address: mausumi.bose@gmail.com (Mausumi Bose)

alternative situation where the location of sensor nodes can be determined prior to deployment, e.g., results by Younis et al. (2006), Martin et al., (2010), Blackburn et al. (2010), Martin et al. (2011), and others. In this paper we focus on the situation of random deployment of nodes.

Several authors have recommended the use of *key predistribution schemes* (KPSs) in a DSN, where secret keys are installed in each sensor node before deployment. Eschenauer and Gligor (2002) pioneered a probabilistic approach to key predistribution and gave a scheme in which every node is assigned a randomly chosen subset of keys from a given pool of keys. Chan et al. (2003) generalized this basic scheme to the q-composite scheme, where two nodes can communicate *only if* they share at least q common keys, where q is a prespecified integer called the *intersection threshold*. Camtepe and Yener (2004) first introduced the use of combinatorial designs in KPSs, using finite projective planes and generalized quadrangles. The principal advantages of using deterministic key assignment schemes based on combinatorial designs compared to random key assignment is that, in the former approach, the problem of generating good pseudorandom numbers is avoided, and moreover, by exploiting the combinatorial structures of the underlying designs, one can study the local connectivity and resiliency properties of the scheme easily, and also carry out shared-key discovery and path-key establishment in a structured manner. For more details on these advantages we refer to Lee and Stinson (2008) and Martin (2009).

Many researchers appreciated the advantages of the above approach and continued to further develop this area. Lee and Stinson (2005a, 2005b) gave a construction based on transversal designs, Chakrabarti et al. (2006) followed this by proposing a merger of a random selection of blocks of a transversal design to form the nodes, Dong et al. (2008) used 3-designs, Ruj and Roy (2007) used partially balanced designs and Ruj et al. (2009) used balanced incomplete block designs in their construction. Lee and Stinson (2008) gave a comprehensive account of key assignment schemes based on combinatorial designs and studied all aspects of their schemes. They gave constructions for two classes of schemes, namely, a linear scheme with intersection threshold $q = 1$ and a quadratic scheme with $q = 2$, based on transversal designs. They studied these two classes of schemes separately and, for each of the two classes, they showed their scheme to be efficient with regard to the levels of connectivity and resiliency, while allowing simple shared-key discovery and path-key establishment. The numbers of nodes required in the network for these two classes of KPSs are of the form p^2 and p^3, respectively, where p is a prime or prime power.

In this paper we propose a new method for constructing KPSs and then study the properties of the resulting schemes. Realizing a connection between the transversal designs used by Lee and Stinson (2008) in their construction for $q = 1$ and a particular type of partially balanced incomplete block designs, we consider the latter designs in their full generality and show that we can construct useful KPSs based on a suitable combination of partially balanced incomplete block designs. We propose one general construction method for any given intersection threshold q (≥ 1), and it will be seen that for the case $q = 1$, our construction covers the linear scheme of Lee and Stinson (2008). One advantage of our proposed method is that it works for all $q(\geq 1)$, and by varying the choices of the designs, one can construct KPSs for networks with varying numbers of nodes, key-pool sizes and numbers of keys per node, thus providing more flexibility in choosing a scheme suitable for the requirements of a situation. For example, now the number of nodes need not be of the particular forms p^2 or p^3, with p prime or prime power, as in Lee and Stinson (2008). These points will be elaborated on in Section 8.

Another advantage of our method of construction is that it allows us to obtain unified and explicit algebraic expressions for the metrics for evaluating the connectivity and resiliency of these schemes, all for general values of $q(\geq 1)$. Using these expressions, the metrics can be easily calculated from the parameters of the particular designs used in the construction. This may be contrasted with Lee and Stinson (2008), Ruj and Roy (2007) or Ruj et al. (2009), where evaluation of the metrics can involve explicit enumeration which may become cumbersome. We also show that our KPSs have good connectivity with high levels of resiliency and the combinatorial structure of the underlying designs make the shared-key discovery and path-key establishment phases particularly simple.

In Section 2 of this paper we give some preliminaries on various metrics for evaluating a KPS, followed by some basics on block designs. Section 3 describes our proposed method for constructing a KPS. Next, in Sections 4 and 5 we obtain expressions for the connectivity and resiliency metrics for these schemes and give illustrative examples. In Section 6 we apply our method to constructions based on some specific block designs, together with numerical illustrations. In Section 7 we discuss how we can label the keys and nodes so that shared-key discovery and path-key establishment become simple. Finally in Section 8 we discuss the gains achieved via our method of construction.

2 Preliminaries

2.1 Some metrics for evaluating KPSs

Several authors have considered some standard metrics for evaluating the performance of key predistribution schemes for distributed sensor networks. We briefly describe these metrics here; a more comprehensive account can be found in Lee and Stinson (2008).

Two basic metrics of a KPS are the *network size* or the number of nodes in the network and the *key storage* or the number of keys stored per node, usually denoted by n and k, respectively. A KPS should typically have large n, say 1000 or much higher and small k, say about 50, though some authors have used k up to 200.

In a DSN the nodes are scattered over a physical area and, since nodes have limited power, each can send or receive signals only over a certain wireless communication range or *neighborhood*. Once the nodes are deployed, any two nodes which are within each other's neighborhood can securely communicate directly with each other if they have at least q common keys, where $q(\geq 1)$ is a specified integer, the *intersection threshold* of the DSN. On the other hand, if two nodes in the same neighborhood do not have q common keys, then they can establish a connection through multiple secure links if there is a sequence of one or more intermediate nodes connecting them such that every pair of adjacent nodes in this sequence share q common keys.

To study the local connectivity of the network, we adopt the metrics used in Lee and Stinson (2005b, 2008), and for this, we now introduce the relevant probabilities as defined by them. Define Pr_1 to be the probability that two random nodes share at least q common keys. Thus given any two randomly chosen nodes within each other's neighborhood, Pr_1 is the probability that these two nodes can establish secure direct communication with each other. Also, define Pr_2 to be the probability that two nodes in the same neighborhood do not have q common keys but there is a third node within the intersection of their neighborhoods which shares q common keys with both of them, thus allowing these two nodes to communicate securely via this third node. So Pr_2 is the probability that two randomly chosen nodes within the same neighborhood fail to establish direct communication but can communicate via a two-hop path. Hence, the sum $\mathrm{Pr} = \mathrm{Pr}_1 + \mathrm{Pr}_2$ is a useful metric for studying the local connectivity of a KPS through either a secure direct link or a secure two-hop path.

Now suppose in an attack on the network a number of sensor nodes are captured at random. Then it is assumed that all keys stored in these compromised nodes are revealed and so cannot

be used for communication any more. Consider any two uncompromised nodes, say A and A', which have at least q common keys. Then the direct communication link between A and A' fails if keys common to them occur in one or more of the compromised nodes; otherwise, the link remains secure. We want the sensor network to be resilient against such random node compromises. From this consideration, resiliency is measured by *fail(s)*, which represents the conditional probability of the link between A and A' to fail when out of the remaining $n-2$ nodes, s randomly chosen ones are compromised, given that A and A' share at least q common keys. A smaller value of fail(s) implies a larger resiliency.

Finally, in order to communicate, two nodes in the same neighborhood need to determine if they share q common keys; this is the *shared-key discovery phase*, and if they do not, then they try to establish a secure two-hop path for communication; this is the *path-key establishment phase*. The difficulties involved in these two phases are also used to assess the utility of a KPS.

2.2 Some basics on block designs

We present some basic definitions of block designs and related concepts which we will need in our constructions of KPSs. Illustrative examples are also given. For more details on these designs we refer to Street and Street (1987), Stinson (2003) and Dey (2010).

Definition 2.1 *A block design d^* is an arrangement of a set of v^* symbols into b^* subsets, these subsets being called blocks.*

Example 2.1 The following is a block design d^* with $v^* = 9$, $b^* = 12$. Denoting the symbols by $1, \ldots, 9$ and blocks by $1, \ldots, 12$, we can write

	Block	*Symbols*	*Block*	*Symbols*	*Block*	*Symbols*	*Block*	*Symbols*
d^* :	1	$4,7,2$	4	$5,8,3$	7	$6,9,1$	10	$1,2,3$
	2	$7,1,5$	5	$8,2,6$	8	$9,3,4$	11	$4,5,6$
	3	$1,4,8$	6	$2,5,9$	9	$3,6,7$	12	$7,8,9$

□

Definition 2.2 *If d^* is a block design with v^* symbols and b^* blocks then its dual design, say d, is a block design obtained from d^* by interchanging the roles of symbols and blocks, i.e., d is a block design involving b^* symbols and v^* blocks, such that the ith block of d contains the jth symbol if and only if the jth block of d^* contains the ith symbol, $1 \le i \le v^*$, $1 \le j \le b^*$.*

Example 2.2 The dual design d obtained from d^* in Example 2.1 has 12 symbols, $1.\ldots,12$ and 9 blocks denoted by $B_1,\ldots,B_9$ as follows:

$$d: \quad \begin{array}{cc||cc||cc} \textit{Block} & \textit{Symbol} & \textit{Block} & \textit{Symbol} & \textit{Block} & \textit{Symbol} \\ B_1 & 2,3,7,10 & B_4 & 1,3,8,11 & B_7 & 1,2,9,12 \\ B_2 & 1,5,6,10 & B_5 & 2,4,6,11 & B_8 & 3,4,5,12 \\ B_3 & 4,8,9,10 & B_6 & 5,7,9,11 & B_9 & 6,7,8,12 \end{array}$$

□

Definition 2.3 *A balanced incomplete block (BIB) design is a block design d^* satisfying the following conditions: (i) each symbol appears at most once in a block, (ii) each block has a fixed number of symbols, say k^*, (iii) each symbol appears in a fixed number of blocks, say r^*, and (iv) every pair of distinct symbols appear together in λ blocks.*

The integer λ is called the concurrence parameter of the BIB design. It can be checked that the design in Example 2.1 is a BIB design with $\lambda = 1$.

Definition 2.4 *A relationship defined on a set of symbols is called an association scheme with two associate classes if it satisfies the following conditions: (a) any two distinct symbols are called either 1st or 2nd associates of each other, any symbol being called the 0th associate of itself, (b) each symbol has θ_j jth associates ($j = 0, 1, 2$), and (c) for every pair of symbols which are jth associates of each other, there are $\phi^j_{u,w}$ symbols that are uth associates of one and wth associates of the other $(j, u, w = 0, 1, 2)$.*

The following relations are evident from Definition 2.4:

$$\theta_0 = 1,\ \phi^1_{0,0} = \phi^1_{0,2} = \phi^1_{2,0} = \phi^2_{0,0} = \phi^2_{1,0} = \phi^2_{0,1} = 0,\ \phi^1_{0,1} = \phi^1_{1,0} = \phi^2_{0,2} = \phi^2_{2,0} = 1. \qquad (1)$$

Various association schemes are available in the literature and for these we refer to Clatworthy (1973). Our construction and results are valid for any general association scheme but in our illustrations in Section 6, we use three of these association schemes, namely group divisible, triangular and Latin square type association schemes. These are defined below.

Definition 2.5 *Let there be af symbols, $(a, f \geq 2)$, partitioned into a groups of f symbols each, and let the symbols in the ith group be denoted by $i1, i2, \ldots, if$, $i = 1, \ldots, a$. A group divisible (GD) association scheme on these af symbols is defined as one where two distinct symbols are called 1st associates if they belong to the same group, and 2nd associates otherwise.*

The above definition implies that for the GD association scheme, in addition to (1) we have $\theta_1 = f-1,\ \theta_2 = f(a-1),\ \phi^1_{1,1} = f-2,\ \phi^1_{1,2} = \phi^1_{2,1} = 0,\ \phi^1_{2,2} = f(a-1),\ \phi^2_{1,1} = 0,\ \phi^2_{1,2} = \phi^2_{2,1} = f-1,\ \phi^2_{2,2} = f(a-2)$.

Example 2.3 Let $a = 2, f = 3$. Then the 6 symbols are partitioned into two groups as: $\{11, 12, 13\},\ \{21, 22, 23\}$. Now, for the symbol 11, the 1st associates are $12, 13$ while its 2nd associates are $21, 22, 23$. Similarly, the 1st and 2nd associates of other symbols may be written down and the parameters of the scheme can be obtained. □

Definition 2.6 *Let there be $\binom{m}{2}$ symbols, $(m \geq 4)$, denoted by ordered pairs ij, $1 \leq i < j \leq m$. A triangular association scheme on these symbols is defined as one where any two distinct symbols are called 1st associates if the ordered pairs representing these symbols have one element in common, and 2nd associates otherwise.*

The above definition implies that for the triangular association scheme, in addition to (1) we have $\theta_1 = 2(m-2), \theta_2 = \binom{m-2}{2},\ \phi^1_{1,1} = m-2, \phi^1_{1,2} = \phi^1_{2,1} = m-3, \phi^1_{2,2} = \binom{m-3}{2}, \phi^2_{1,1} = 4, \phi^2_{1,2} = \phi^2_{2,1} = 2m-8, \phi^2_{2,2} = \binom{m-4}{2}$.

Example 2.4 Let $m = 5$. The $\binom{5}{2}$ $(= 10)$ symbols are denoted by the ordered pairs: $12, 13, 14, 15, 23, 24, 25, 34, 35, 45$. Now, for the symbol 12, the 1st associates are $13, 14, 15, 23, 24, 25$ while its 2nd associates are $34, 35, 45$. Similarly, the 1st and 2nd associates of other symbols may be written down and the parameters of the scheme obtained. □

Definition 2.7 *Let there be p^2 symbols, $p \geq 3$, arranged in a $p \times p$ square $\mathcal{S}$ and suppose $k-2$ mutually orthogonal Latin squares of order p are available. A Latin square type association scheme on these p^2 symbols is defined as one where any two distinct symbols are called 2nd associates if they occur in the same row or same column of $\mathcal{S}$ or if, after superimposing each of the Latin squares on $\mathcal{S}$, they occur in positions occupied by the same letter in any of the Latin squares. Otherwise, they are called 1st associates.*

The above definition implies that for the Latin square type association scheme, in addition to (1) we have $\theta_1 = (p-1)(p-k+1),\ \theta_2 = k(p-1),\ \phi^1_{1,1} = (p-k)(p-k-1)+p-2,\ \phi^1_{1,2} = \phi^1_{2,1} = k(p-k),\ \phi^1_{2,2} = k(k-1),\ \phi^2_{1,1} = (p-k)(p-k+1),\ \phi^2_{1,2} = \phi^2_{2,1} = (k-1)(p-k+1),\ \phi^2_{2,2} = (k-1)(k-2)+p-2$.

Example 2.5 Let $p = 4$ and $k = 3$. We denote the 4^2 $(= 16)$ symbols by the ordered pairs: $11, 12, 13, 14, 21, 22, \ldots, 43, 44$ and write $\mathcal{S}$ and the single Latin square $\mathcal{L}$ as

$$\mathcal{S} = \begin{array}{cccc} 11 & 12 & 13 & 14 \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{array}, \qquad \mathcal{L} = \begin{array}{cccc} A & B & C & D \\ B & C & D & A \\ C & D & A & B \\ D & A & B & C. \end{array}$$

Then it follows that for the symbol 11, the 2nd associates are $12, 13, 14, 21, 31, 41, 24, 33, 42$, while its 1st associates are $22, 23, 32, 34, 43, 44$. Similarly, the 1st and 2nd associates of other symbols may be written down and the parameters of the scheme obtained. □

Definition 2.8 *Given an association scheme with two associate classes on a set of v^* symbols, a partially balanced incomplete block (PBIB) design based on this association scheme is a block design d^* with v^* symbols and b^* blocks satisfying the following conditions: (i) each symbol appears at most once in a block, (ii) each block has a fixed number of symbols, say k^*, (iii) each symbol appears in a fixed number of blocks, say r^*, and (iv) every pair of symbols which are jth associates of each other appear together in λ_j blocks $(j = 1, 2)$.*

The integers λ_1 and λ_2 are the two concurrence parameters of the PBIB design, where $\lambda_1 \neq \lambda_2$.

Example 2.6 We can construct a PBIB design d^* based on the GD association scheme by pairing each of the af symbols with its second associates to form the blocks. Thus, such a design can be constructed for every integer $a, f(\geq 2)$. It is easy to see that this design will have $v^* = af,\ b^* = \binom{a}{2}f^2,\ k^* = 2,\ r^* = (a-1)f$ and $\lambda_1 = 0,\ \lambda_2 = 1$. For example, a PBIB design based on the GD association scheme in Example 2.3 can be constructed by pairing each of the 6 symbols with its second associates to get 9 blocks as follows:

$$d^*: \begin{array}{cc||cc||cc} \textit{Block} & \textit{Symbol} & \textit{Block} & \textit{Symbol} & \textit{Block} & \textit{Symbol} \\ 1 & 11, 21 & 4 & 12, 21 & 7 & 13, 21 \\ 2 & 11, 22 & 5 & 12, 22 & 8 & 13, 22 \\ 3 & 11, 23 & 6 & 12, 23 & 9 & 13, 23 \end{array}.$$

Clearly, this GD design has $v^* = 6,\ b^* = 9,\ k^* = 2,\ r^* = 3,\ \lambda_1 = 0,\ \lambda_2 = 1$. □

Example 2.7 We can construct a PBIB design d^* based on the triangular association scheme by pairing each of the $\binom{m}{2}$ symbols with its second associates to get the blocks. Thus, such a

design can be constructed for every $m \geq 4$. It is easy to see that this design will have $v^* = \binom{m}{2}$, $b^* = 3\binom{m}{4}$, $k^* = 2$, $r^* = \binom{m-2}{2}$, and $\lambda_1 = 0$, $\lambda_2 = 1$. For example, a PBIB design based on the triangular association scheme in Example 2.4 has 10 symbols arranged in 15 blocks given by: $(12, 34), (12, 35), (12, 45), (13, 24), (13, 25), (13, 45)$, etc. □

For a given positive integer $t(\geq 1)$, we now consider t block designs $d_1^*, \ldots, d_t^*$ such that each d_i^* is a PBIB design based on an association scheme with two associate classes and concurrence parameters $\lambda_1 = 0$, $\lambda_2 = 1$, the common occurrence number of every symbol in d_i^* $(i = 1, \ldots, t)$ being at least t. For $1 \leq i \leq t$, consider the dual d_i of d_i^* and denote the symbols of d_i by $1(i), \ldots, v_i(i)$, and blocks by $B_1(i), \ldots, B_{b_i}(i)$. Then from Definitions 2.2 and 2.8, it is evident that each such d_i, involving v_i symbols and b_i blocks, satisfies the following conditions:
(I) every symbol occurs at most once in each block of d_i,
(II) every symbol occurs in a fixed number of blocks, say r_i $(2 \leq r_i < b_i)$, of d_i,
(III) every block of d_i contains a fixed number of symbols, say k_i $(v_i > k_i \geq t)$, and
(IV) there is an association scheme with two associate classes *on the set of blocks* of d_i; any two distinct blocks either have no common symbol, in which case they are called 1st associates of each other; or they have exactly one symbol in common, in which case they are called 2nd associates of each other; every block being its own 0th associate.

For $1 \leq i \leq t$, let $\theta_j(i)$ denote the number of jth associates of any block of d_i, and given any two blocks which are jth associates of each other, let $\phi_{u,w}^j(i)$ denote the number of blocks of d_i which are uth associates of one and wth associates of the other $(j, u, w = 0, 1, 2)$. Then clearly, for each design d_i the relations corresponding to (1) hold, and moreover,

$$\theta_0(i) = 1, \quad \theta_1(i) + \theta_2(i) = b_i - 1 \text{ and } \theta_1(i) > 0, \quad \theta_2(i) > 0 \ (1 \leq i \leq t). \tag{2}$$

Example 2.8 Let d_1^* be the PBIB design given in Example 2.6. Then, the dual of d_1^* is given by a design d_1 with 6 symbols arranged in 9 blocks. Denoting these symbols as $1(1), \ldots, 9(1)$ and the blocks as $B_1(1), \ldots, B_6(1)$ as described above, the design d_1 has blocks given by:

	Block	Symbols	Block	Symbols	Block	Symbols
d_1 :	$B_1(1)$	$1(1), 2(1), 3(1)$	$B_3(1)$	$7(1), 8(1), 9(1)$	$B_5(1)$	$2(1), 5(1), 8(1)$
	$B_2(1)$	$4(1), 5(1), 6(1)$	$B_4(1)$	$1(1), 4(1), 7(1)$	$B_6(1)$	$3(1), 6(1), 9(1)$

Clearly, d_1 satisfies conditions (I)-(III) above with $v_1 = 9$, $b_1 = 6$, $r_1 = 2$, $k_1 = 3$. Also,

condition (IV) is satisfied; we have the following association structure:

Block	1st associates	2nd associates
$B_1(1)$	$B_2(1), B_3(1)$	$B_4(1), B_5(1), B_6(1)$
$B_2(1)$	$B_1(1), B_3(1)$	$B_4(1), B_5(1), B_6(1)$
$B_3(1)$	$B_1(1), B_2(1)$	$B_4(1), B_5(1), B_6(1)$
$B_4(1)$	$B_5(1), B_6(1)$	$B_1(1), B_2(1), B_3(1)$
$B_5(1)$	$B_4(1), B_6(1)$	$B_1(1), B_2(1), B_3(1)$
$B_6(1)$	$B_4(1), B_5(1)$	$B_1(1), B_2(1), B_3(1)$

So, in addition to the relations in (1), we have $\theta_1(1) = 2,\ \theta_2(1) = 3,\ \phi^1_{1,1}(1) = 1,\ \phi^1_{1,2}(1) = \phi^1_{2,1}(1) = 0,\ \phi^1_{2,2}(1) = 3,\ \phi^2_{1,1}(1) = 0,\ \phi^2_{1,2}(1) = \phi^2_{2,1}(1) = 2,\ \phi^2_{2,2}(1) = 0.$ □

In the above development, we can as well take any d_i^* to be a BIB design with $\lambda = 1$, each symbol appearing at least t times in the design. Then by Definitions 2.2 and 2.3, its dual design d_i will again satisfy the conditions (I)-(IV), but with $\theta_1(i) = 0$. This is because in this case, any two blocks of d_i will always have exactly one symbol in common and so by (IV), any two distinct blocks of d_i can only be second associates, there being no 1st associates for any block. Thus, conditions (1) and (2) are valid, keeping in mind that now in (2), $\theta_1(i) = 0$ and in (1), the quantities $\phi^1_{u,w}(i)$ do not arise, while $\phi^0_{u,w}(i) = 0$ and $\phi^2_{u,w}(i) = 0$ whenever $u = 1$ or $w = 1$.

Example 2.9 Let d_2^* be the BIB design in Example 2.1. Then, the dual of d_2^* is the design in Example 2.2, denoted by d_2, say. Clearly, d_2 satisfies conditions (I)-(III) with $v_2 = 12, b_2 = 9, r_2 = 3,\ k_2 = 4$. Also, condition (IV) is satisfied with no block in d_2 having any other block as its 1st associate, all distinct blocks being 2nd associates of each other. Thus, in addition to the relations in (1), we have $\theta_1(2) = 0,\ \theta_2(2) = 8,\ \phi^2_{1,1}(2) = \phi^2_{1,2}(2) = \phi^2_{2,1}(2) = 0,\ \phi^2_{2,2}(2) = 7.$ □

In view of the above discussion, define two sets Q and $\bar{Q}$ as

$$Q = \{i : 1 \le i \le t,\, \theta_1(i) > 0\} \text{ and } \bar{Q} = \{i : 1 \le i \le t,\, \theta_1(i) = 0\}. \tag{3}$$

Clearly, $i \in Q$ if d_i^* is a PBIB design and $i \in \bar{Q}$ if d_i^* is a BIB design as indicated above.

3 Construction of KPS

Suppose the intersection threshold of the required KPS is stipulated as q. We consider $t = q$ block designs $d_i^*, 1 \le i \le t$, where each d_i^* is either a PBIB design with $\lambda_1 = 0, \lambda_2 = 1$ or a

BIB design with $\lambda = 1$; every symbol appearing at least t times in each design. As before, for $1 \leq i \leq t$, let d_i be the dual of design d_i^*, so d_i satisfies conditions (I)-(IV) listed in Subsection 2.2. A KPS with $q = t$, based on the designs $d_1, \ldots, d_t$ is constructed as follows.

First identify the symbols in $d_1, \ldots, d_t$ as the keys of the KPS. Next, consider all possible selections of one block from each d_i, $1 \leq i \leq t$, and take the union of the t blocks in each such selection as a node of the KPS. Thus the resulting KPS has $v = \sum_{i=1}^{t} v_i$ keys given by the symbols $1(i), \ldots, v_i(i), (1 \leq i \leq t)$ and $n = \Pi_{i=1}^{t} b_i$ nodes given by

$$N(\alpha_1 \ldots \alpha_t) = B_{\alpha_1}(1) \cup \cdots \cup B_{\alpha_t}(t), \quad 1 \leq \alpha_i \leq b_i, \quad 1 \leq i \leq t. \tag{4}$$

By condition (III) in Subsection 2.2, every node has $k = \sum_{i=1}^{t} k_i$ keys. Note that n is multiplicative in the b_i while k is additive in the $k_i, 1 \leq i \leq t$. As illustrated later, this helps in attaining the twin objectives of having a large number of nodes in the network while keeping the number of keys stored per node relatively small.

Remark 3.1 One of the two constructions in Lee and Stinson (2008), namely, the one with $q = 1$, is covered by (4). This fact will be elucidated in more detail in Remarks 4.3 and 5.3. □

For $1 \leq i \leq t$, it is clear from (4) that the block $B_{\alpha_i}(i)$ is the contribution of the design d_i to the node $N(\alpha_1 \ldots \alpha_t)$. From this perspective, we introduce the following definition.

Definition 3.1 *When nodes are constructed as in (4), the block of d_i that appears in any node A is called the projection of the node A on the design d_i and is denoted by $proj(A, i)$.*

Thus from (4), $B_{\alpha_i}(i)$ is the projection of the node $N(\alpha_1 \ldots \alpha_t)$ on d_i. We now define an association scheme on the set of nodes as given by (4). This will play a crucial role in exploring the properties of the KPSs obtained through (4). Here each associate relationship is represented by a t-tuple of the form $j_1 \ldots j_t$.

Definition 3.2 *Two distinct nodes A and A' are $j_1 \ldots j_t$th associates of each other if, for $1 \leq i \leq t$, $proj(A, i)$ and $proj(A', i)$ are j_ith associates of each other.*

We illustrate the above ideas with a small toy example below.

Example 3.1 *Toy Example:* Let $q = 2$. So, by the above method, we take $t = 2$ and construct a KPS with $q = 2$ based on two designs, d_1^* and d_2^*. Let us take d_1^* as the PBIB design given

in Example 2.6 and d_2^* as the BIB design in Example 2.1. Their respective duals d_1 and d_2 are given in Examples 2.8 and 2.2. The KPS constructed by the above method has $n = b_1 b_2 = 54$ nodes with $k = k_1 + k_2 = 7$ keys per node. Using (4), we get the key assignments in the nodes, for example, two typical nodes are:

$N(1,1) = B_1(1) \cup B_1(2) = 1(1), 2(1), 3(1), 2(2), 3(2), 7(2), 10(2)$, and

$N(3,4) = B_3(1) \cup B_4(2) = 7(1), 8(1), 9(1), 1(2), 3(2), 8(2), 11(2)$.

Then, by Definition 3.1, the blocks $B_1(1)$ and $B_1(2)$ are the projections of the node $N(1,1)$ on the designs d_1 and d_2, respectively, i.e., $proj(N(1,1),1) = B_1(1)$ and $proj(N(1,1),2) = B_1(2)$. Similarly, $proj(N(3,4),1) = B_3(1)$ and $proj(N(3,4),2) = B_4(2)$. Now, from Examples 2.8 and 2.9, we see that $B_1(1)$ and $B_3(1)$ are 1st associates while $B_1(2)$ and $B_4(2)$ are 2nd associates. So, by Definition 3.2 we say that nodes $N(1,1)$ and $N(3,4)$ are 12th associates of each other. □

In Definition 3.2, $j_1 \dots j_t \neq 0 \dots 0$, since the nodes A and A' are distinct. Also, by (3), $j_i = 0, 1$ or 2 if $i \in Q$ and $j_i = 0$ or 2 if $i \in \bar{Q}$. Thus the set of all possible associate relationships between two distinct nodes in the KPS is given by

$$I = \{j_1 \dots j_t : j_1 \dots j_t \neq 0 \dots 0;\ j_i = 0, 1 \text{ or } 2 \text{ if } i \in Q \text{ and } j_i = 0 \text{ or } 2 \text{ if } i \in \bar{Q}\}. \tag{5}$$

We now obtain expressions for certain parameters of the association scheme on the set of nodes, as given by Definition 3.2. For $j_1 \dots j_t \in I$, let $n_{j_1 \dots j_t}$ denote the number of $j_1 \dots j_t$th associates of any node A. Then by Definition 3.2, $n_{j_1 \dots j_t}$ equals the product, over $1 \leq i \leq t$, of the number of j_ith associates of $proj(A,i)$. Therefore,

$$n_{j_1 \dots j_t} = \prod_{i=1}^{t} \theta_{j_i}(i). \tag{6}$$

Again, given any two nodes which are $j_1 \dots j_t$th associates of each other, let $p^{j_1 \dots j_t}_{u_1 \dots u_t, w_1 \dots w_t}$ denote the number of nodes that are $u_1 \dots u_t$th associates of one node and $w_1 \dots w_t$th associates of the other, where $j_1 \dots j_t, u_1 \dots u_t$ and $w_1 \dots w_t \in I$. Then as in (6),

$$p^{j_1 \dots j_t}_{u_1 \dots u_t, w_1 \dots w_t} = \prod_{i=1}^{t} \phi^{j_i}_{u_i, w_i}(i). \tag{7}$$

Let $\lambda_{j_1 \dots j_t}$ denote the number of common keys between any two distinct nodes A and A' which are $j_1 \dots j_t$th associates of each other, $j_1 \dots j_t \in I$. Then from Definition 3.2 it follows that

$$\lambda_{j_1 \dots j_t} = \sum_{i=1}^{t} \psi_{j_i}(i) \tag{8}$$

where $\psi_{j_i}(i)$ is the number of symbols (or equivalently, keys) common to $proj(A, i)$ and $proj(A', i)$ when they are j_ith associates of each other. By condition (IV) of Subsection 2.2 and the fact that each block of d_i is the 0th associate of itself, it is evident that

$$\psi_0(i) = k_i, \;\; \psi_1(i) = 0, \;\; \psi_2(i) = 1, \;\; 1 \leq i \leq t. \tag{9}$$

We illustrate these concepts by continuing with the toy example in Example 3.1.

Example 3.2 *Toy Example continued:* Since d_1^* is a PBIB and d_2^* a BIB design, by (5), the set of all possible associate relationships between any two nodes in the KPS is $I = \{02, 10, 12, 20, 22\}$. Now, Examples 2.8 and 2.9 show that $\theta_1(1) = 2,\ \theta_2(1) = 3$ and $\theta_2(2) = 8$. Recalling from (1) that $\theta_0(1) = \theta_0(2) = 1$, by (6) it follows that the number of 02th associates of any node in the KPS is $n_{02} = 1 \times 8 = 8$. Similarly, $n_{10} = 2,\ n_{12} = 16,\ n_{20} = 3,\ n_{22} = 24$. Now, using the values of $\phi^{j_1}_{u_1,w_1}(1)$ and $\phi^{j_2}_{u_2,w_2}(2)$ from Examples 2.8 and 2.9 and remembering (1), it follows from (7) that $p^{12}_{02,10} = \phi^1_{01}(1)\phi^2_{20}(2) = 1 \times 1 = 1 = p^{12}_{10,02}$, and similarly, $p^{12}_{22,20} = p^{12}_{20,22} = 3 \times 1 = 3,\ p^{12}_{22,22} = 3 \times 7 = 21,\ p^{12}_{02,12} = p^{12}_{12,02} = 1 \times 7 = 7,\ p^{12}_{10,12} = p^{12}_{12,10} = 1 \times 1 = 1,\ p^{12}_{12,12} = 1 \times 7 = 7$, while every other $p^{12}_{u_1u_2,w_1w_2}$ equals zero.

Again, by (9), $\psi_0(1) = 3,\ \psi_0(2) = 4,\ \psi_1(1) = 0,\ \psi_2(1) = \psi_2(2) = 1$, and so it follows from (8) that the number of symbols common between any two nodes which are 02th associates of each other is $\lambda_{02} = 3 + 1 = 4$. Similarly, $\lambda_{10} = 4,\ \lambda_{12} = 1, \lambda_{20} = 5, \lambda_{22} = 2$. Hence, since $q = 2$, all pairs of nodes, other than those which are 12th associates of each other, can communicate directly with one another. □

4 Local connectivity

In this section we explore the local connectivity of the KPS introduced in (4). Theorem 4.1 is the main result in this section and it gives an expression for the metric Pr for this scheme, in terms of the parameters of the constituent designs. Some notation and two lemmas are needed in order to present the theorem. Let

$$\Delta = \{j_1 \dots j_t : j_1 \dots j_t \in I,\ \lambda_{j_1 \dots j_t} \geq q\}, \tag{10}$$

where I is given by (5). So, any two nodes which are $j_1 \dots j_t$th associates of each other can communicate directly only if $j_1 \dots j_t \in \Delta$. Let $\bar{\Delta}$ be the complement of Δ in I and let $\sum_\Delta$, $\sum_{\bar{\Delta}}$ and $\sum_I$ stand for sums over $j_1 \dots j_t \in \Delta$, $j_1 \dots j_t \in \bar{\Delta}$ and $j_1 \dots j_t \in I$, respectively.

Given two distinct nodes which are $j_1 \dots j_t$th associates of each other, let $\mu_{j_1 \dots j_t}$ denote the number of nodes sharing at least $q(= t)$ common keys with both of them. Also, for any two distinct nodes A and A' in each other's neighborhood, let the intersection of their neighborhoods contain η nodes excluding A and A' themselves. Define

$$\beta_{j_1 \dots j_t} = 1 - \frac{\binom{n-2-\mu_{j_1 \dots j_t}}{\eta}}{\binom{n-2}{\eta}}, \quad j_1 \dots j_t \in \bar{\Delta}. \tag{11}$$

Lemma 4.1 *Any $j_1 \dots j_t$ $(\in I)$ is a member of Δ if and only if either*
(a) $j_i = 0$ for at least one i, or (b) $j_1 = \dots = j_t = 2$.

Proof of Lemma 4.1 Follows from (8), (9) and (10), noting that $k_i \geq t$ for each i by condition (III) of Subsection 2.2. □

Lemma 4.2 *Given two distinct nodes which are $j_1 \dots j_t$th associates of each other, if $j_1 \dots j_t \in \bar{\Delta}$, then $\mu_{j_1 \dots j_t} = \sum\sum p^{j_1 \dots j_t}_{u_1 \dots u_t, w_1 \dots w_t}$, the double sum being over $u_1 \dots u_t \in \Delta$ and $w_1 \dots w_t \in \Delta$.*

Proof of Lemma 4.2 Follows from (10), on recalling the definition of $p^{j_1 \dots j_t}_{u_1 \dots u_t, w_1 \dots w_t}$. □

Theorem 4.1 *The probability that two distinct randomly chosen nodes A and A' in each other's neighborhood can establish communication, either directly or via a two-hop path, equals* $\Pr = \Pr_1 + \Pr_2$, *where*

$$\Pr_1 = \frac{\sum_{\Delta} n_{j_1 \dots j_t}}{n-1}\,, \tag{12}$$

and

$$\Pr_2 = \sum_{\bar{\Delta}} \frac{n_{j_1 \dots j_t}}{n-1} \beta_{j_1 \dots j_t} \approx \sum_{\bar{\Delta}} \frac{n_{j_1 \dots j_t}}{n-1} \left[1 - \left(1 - \frac{\mu_{j_1 \dots j_t}}{n-2} \right)^{\eta} \right]. \tag{13}$$

Proof of Theorem 4.1 Let C be the event that the nodes A and A' can establish communication either directly or via a two-hop path. Define $E(j_1 \dots j_t)$ as the event that A and A' are $j_1 \dots j_t$th associates of each other. Since the events $E(j_1 \dots j_t),\ j_1 \dots j_t \in I$, are mutually exclusive and exhaustive, we can write

$$\Pr = P(C) = \sum_{I} P\{E(j_1 \dots j_t)\} P\{C | E(j_1 \dots j_t)\}, \tag{14}$$

where $P\{C|E(j_1 \dots j_t)\}$ is, as usual, the conditional probability of C, given $E(j_1 \dots j_t)$. Now, for each $j_1 \dots j_t \in I$, recalling that there are $n_{j_1 \dots j_t}$ nodes which are $j_1 \dots j_t$th associates of any given node, it follows that

$$P\{E(j_1 \dots j_t)\} = \frac{\frac{1}{2} n \times n_{j_1 \dots j_t}}{\binom{n}{2}} = \frac{n_{j_1 \dots j_t}}{n-1}. \tag{15}$$

Moreover, if $j_1 \dots j_t \in \Delta$, then by (10), A and A' have at least t common keys and hence can establish direct communication, implying

$$P\{C|E(j_1 \dots j_t)\} = 1, \text{ for } j_1 \dots j_t \in \Delta. \tag{16}$$

On the other hand, if $j_1 \dots j_t \in \bar{\Delta}$, then they have less than t common keys. In this case, direct communication between A and A' is not possible but they can establish communication via a two-hop path provided the intersection of their neighborhoods contains one of the $\mu_{j_1 \dots j_t}$ nodes sharing at least t common keys with both of them. Hence, using (11), it is clear that

$$P\{C|E(j_1 \dots j_t)\} = \beta_{j_1 \dots j_t}, \text{ for } j_1 \dots j_t \in \bar{\Delta}. \tag{17}$$

Substitution of (15), (16) and (17) in (14) establishes the theorem. □

Remark 4.1 The approximation used in (13) is quite accurate when the quantities $n - 2 - \mu_{j_1,\dots,j_t}$ are large relative to η, which is typically the case. Note also that the expression for $\Pr_2$ in (13) is a refinement of that used in Lee and Stinson (2008) for $q = 2$. To see this, first note from (12) that

$$\frac{\sum_{\bar{\Delta}} n_{j_1 \dots j_t}}{n-1} = \frac{n - 1 - \sum_{\Delta} n_{j_1 \dots j_t}}{n-1} = 1 - \Pr_1, \tag{18}$$

because $\sum_I n_{j_1 \dots j_t} = n - 1$. Next, write $\mu^* = \min\{\mu_{j_1 \dots j_t} : j_1 \dots j_t \in \bar{\Delta}\}$ and from (11) observe that $\beta_{j_1 \dots j_t} \geq \beta^*$ for every $j_1 \dots j_t \in \bar{\Delta}$, where β^* is defined as in (11) with $\mu_{j_1 \dots j_t}$ replaced by μ^*. As a result, from (13) and (18), we get

$$\Pr_2 \geq \sum_{\bar{\Delta}} \frac{n_{j_1 \dots j_t}}{n-1} \beta^* = (1 - \Pr_1)\beta^* \approx (1 - \Pr_1) \left[1 - \left(1 - \frac{\mu^*}{n-2} \right)^{\eta} \right]. \tag{19}$$

For their quadratic scheme, Lee and Stinson (2008) took $\Pr_2$ as the counterpart of the lower bound in (19) for their setup. Instead, we work here with the more direct expression given in (13), and in addition, this is valid for all $q \geq 1$. □

Remark 4.2 Lee and Stinson (2008) remarked that it is difficult to find an algebraic expression of μ^* for their quadratic KPS, and therefore, studied $\Pr_2$ through design specific numerical evaluation of μ^*. An advantage of our method is that for all $q(\geq 1)$, even when one starts with arbitrary designs, Theorem 4.1 gives readily applicable algebraic expressions for both $\Pr_1$ and $\Pr_2$ for our schemes in terms of the design parameters. Equations (2), (6), (7), and Lemmas 4.1 and 4.2 can be used in finding the $n_{j_1 \dots j_t}$ and $\mu_{j_1 \dots j_t}$, and hence one can find $\Pr_1$ and $\Pr_2$ explicitly in specific situations. The following examples serve to illustrate this point for the cases $q = 1$ and $q = 2$. □

Example 4.1 Case: $q = 1$. We take $t = 1$ and construct a KPS as in (4) with d_1^* either (a) a PBIB or (b) a BIB design.

(a) If d_1^* is a PBIB design with $\lambda_1 = 0, \lambda_2 = 1$, then its dual design d_1 has $\theta_1(1) > 0$. Then $n = b_1$ and by (3), (5) and Lemma 4.1, $Q = \{1\}$, $I = \{1, 2\}$, $\Delta = \{2\}$ and $\bar{\Delta} = \{1\}$. Also, from (6) and (7), $n_1 = \theta_1(1)$, $n_2 = \theta_2(1)$ and $p_{2,2}^1 = \phi_{2,2}^1(1)$. So by Lemma 4.2, $\mu_1 = p_{2,2}^1 = \phi_{2,2}^1(1)$. Hence (12) and (13) yield

$$\Pr_1 = \frac{\theta_2(1)}{b_1 - 1} \quad \text{and} \quad \Pr_2 \approx \frac{\theta_1(1)}{b_1 - 1} \left[1 - \left(1 - \frac{\phi_{2,2}^1(1)}{b_1 - 2} \right)^{\eta} \right]. \tag{20}$$

(b) If d_1^* is a BIB design with $\lambda = 1$, then its dual d_1 has $\theta_1(1) = 0$, $\theta_2(1) = b_1 - 1$. Then $n = b_1$ and by (3), (5) and Lemma 4.1, $\bar{Q} = \{1\}$, $I = \{2\} = \Delta$. So by (12), $\Pr_1 = \frac{b_1 - 1}{b_1 - 1} = 1$ always. □

Remark 4.3 As mentioned in the Remark 3.1, the construction in Lee and Stinson (2008) with $q = 1$ is covered by (4). To see this in detail, we first note that in their construction, the nodes are taken as the blocks of a transversal design (cf. Stinson (2003)), with kp symbols and p^2 blocks, such that (a) the set of symbols is partitioned into k groups each of cardinality p, (b) each group contributes one symbol to each block, and (c) any two symbols from different groups occur together in exactly one block.

Recalling Definitions 2.7 and 2.8 it can now be checked that such a transversal design is actually the dual of a PBIB design based on a Latin square type association scheme with $v^* = p^2, b^* = kp, r^* = k, k^* = p$, and $\lambda_1 = 0, \lambda_2 = 1$. Hence one can verify that their construction can equivalently be described via our construction in (4) with $t = 1$ and d_1^* chosen as this PBIB design. Then its dual d_1 is their transversal design involving $v_1 = kp$ symbols and $b_1 = p^2$ blocks, such that conditions (I)–(IV) of Subsection 2.2 hold with $r_1 = p$, $k_1 = k$, $\theta_1(1) = (p-1)(p+1-k)$, $\theta_2(1) = k(p-1)$, $\phi_{2,2}^1(1) = k(k-1)$. Hence we can apply (20) to get

$$\Pr_1 = \frac{k}{p+1} \quad \text{and} \quad \Pr_2 \approx \left(1 - \frac{k}{p+1} \right) \left[1 - \left(1 - \frac{k(k-1)}{p^2 - 2} \right)^{\eta} \right].$$

These exactly match the expressions for $\Pr_1$ and $\Pr_2$ in Subsection 4.1.1 of Lee and Stinson (2008). We will see in Remark 5.3 that their expression for fail(s) also follow from our corresponding expressions. □

Example 4.2 Case: $q = 2$. *Toy example:* We continue with the KPS considered in Examples 3.1 and 3.2. From the $\lambda_{j_1 j_2}$ values in Example 3.2, it follows that $\Delta = \{02, 10, 20, 22\}$ and so, using the $n_{j_1 j_2}$ values obtained there, (12) gives $\Pr_1 = (8 + 2 + 3 + 24)/53 = 0.6981$. To

obtain Pr_2, we see that $\bar{\Delta} = \{12\}$, and so, remembering the values of $p^{12}_{u_iu_2,w_1w_2}, u_1u_2, w_1w_2 \in \Delta$, obtained in Example 3.2, it follows from Lemma 4.2 that $\mu_{12} = 1+1+3+3+21 = 29$. Hence, from (13), $\mathrm{Pr}_2 = \frac{16}{53}[1-(1-29/52)^\eta]$ and for varying values of η we have

η	1	2	3	4	5	10	15	20
$\mathrm{Pr}_1 + \mathrm{Pr}_2$	0.8665	0.9409	0.9739	0.9884	0.9949	0.9999	1.0000	1.0000

□

Example 4.3 General Case, $q = 2$: (a) PBIB and BIB design: Suppose we construct a KPS as in (4) based on two designs d_1^* and d_2^* given by a PBIB design with $\lambda_1 = 0, \lambda_2 = 1$ and a BIB design with $\lambda = 1$, respectively. Hence their duals d_1 and d_2 have $\theta_1(1) > 0$ and $\theta_1(2) = 0$. Then $n = b_1b_2$ and by (3), (5) and Lemma 4.1, we have $Q = \{1\}$, $\bar{Q} = \{2\}$, $I = \{02, 10, 12, 20, 22\}$, $\Delta = \{02, 10, 20, 22\}$ and $\bar{\Delta} = \{12\}$. Also, by (2) and (6), $n_{02} = \theta_2(2)$, $n_{10} = \theta_1(1)$, $n_{12} = \theta_1(1)\theta_2(2)$, $n_{20} = \theta_2(1)$ and $n_{22} = \theta_2(1)\theta_2(2)$. So from (12), on using (2), we have

$$\begin{aligned} \mathrm{Pr}_1 &= \frac{1}{b_1b_2-1}\{\theta_2(2)+\theta_1(1)+\theta_2(1)+\theta_2(1)\theta_2(2)\}, \\ &= \frac{1}{b_1b_2-1}\{b_1+b_2-2+\theta_2(1)\theta_2(2)\}. \end{aligned} \tag{21}$$

Next by (7) and Lemma 4.2,

$$\begin{aligned} \mu_{12} &= \sum\sum p^{12}_{u_1u_2,w_1w_2} = \sum\sum \phi^1_{u_1,w_1}(1)\phi^2_{u_2,w_2}(2) \\ &= \phi^1_{0,0}(1)\phi^2_{2,2}(2) + \phi^1_{0,1}(1)\phi^2_{2,0}(2) + \phi^1_{0,2}(1)\phi^2_{2,0}(2) + \phi^1_{0,2}(1)\phi^2_{2,2}(2) \\ &\quad + \phi^1_{1,0}(1)\phi^2_{0,2}(2) + \phi^1_{1,1}(1)\phi^2_{0,0}(2) + \phi^1_{1,2}(1)\phi^2_{0,0}(2) + \phi^1_{1,2}(1)\phi^2_{0,2}(2) \\ &\quad + \phi^1_{2,0}(1)\phi^2_{0,2}(2) + \phi^1_{2,1}(1)\phi^2_{0,0}(2) + \phi^1_{2,2}(1)\phi^2_{0,0}(2) + \phi^1_{2,2}(1)\phi^2_{0,2}(2) \\ &\quad + \phi^1_{2,0}(1)\phi^2_{2,2}(2) + \phi^1_{2,1}(1)\phi^2_{2,0}(2) + \phi^1_{2,2}(1)\phi^2_{2,0}(2) + \phi^1_{2,2}(1)\phi^2_{2,2}(2). \end{aligned}$$

Hence invoking (1) for the association schemes underlying the designs d_1 and d_2, we get

$$\mu_{12} = 2 + 2\phi^1_{1,2}(1) + 2\phi^1_{2,2}(1) + \phi^1_{2,2}(1)\phi^2_{2,2}(2). \tag{22}$$

Since $\bar{\Delta} = \{12\}$ and $n_{12} = \theta_1(1)\theta_2(2)$, (13) now yields

$$\mathrm{Pr}_2 \approx \frac{\theta_1(1)\theta_2(2)}{b_1b_2-1}\left[1-\left(1-\frac{\mu_{12}}{b_1b_2-2}\right)^\eta\right], \tag{23}$$

with μ_{12} as given in (22). □

Example 4.4 General Case $q = 2$: (b) Both PBIB designs: Now suppose we construct a KPS as in (4) based on two PBIB designs, each with $\lambda_1 = 0$ and $\lambda_2 = 1$, resulting in $\theta_1(1)$ and $\theta_1(2)$ both positive. Then $n = b_1 b_2$ and by (3), (5) and Lemma 4.1, $Q = \{1, 2\}, I = \{01, 02, 10, 11, 12, 20, 21, 22\}$, $\Delta = \{01, 02, 10, 20, 22\}$ and $\bar{\Delta} = \{11, 12, 21\}$. Hence proceeding as in Example 4.3, one can check that

$$\begin{aligned}
\Pr_1 &= \frac{1}{b_1 b_2 - 1}\{b_1 + b_2 - 2 + \theta_2(1)\theta_2(2)\}, \\
n_{11} &= \theta_1(1)\theta_1(2),\ n_{12} = \theta_1(1)\theta_2(2),\ n_{21} = \theta_2(1)\theta_1(2) \\
\mu_{11} &= 2 + \phi^1_{2,2}(1)\phi^1_{2,2}(2),\ \ \mu_{12} = 2 + 2\phi^1_{1,2}(1) + 2\phi^1_{2,2}(1) + \phi^1_{2,2}(1)\phi^2_{2,2}(2), \\
\mu_{21} &= 2 + 2\phi^1_{1,2}(2) + 2\phi^1_{2,2}(2) + \phi^2_{2,2}(1)\phi^1_{2,2}(2).
\end{aligned}$$

$\Pr_2$ can be readily obtained using these expressions for the $n_{j_1 j_2}$ and $\mu_{j_1 j_2}$, $j_1 j_2 \in \bar{\Delta}$, in (13). □

5 Resiliency

We now study the resiliency of the KPS as given by (4) and for this we recall the notion of fail(s) introduced in Subsection 2.1. Theorem 5.1 below gives an algebraic expression for fail(s) and it is the main result of this section. Some notation and a lemma are needed in order to present the theorem.

Let A and A' be two distinct nodes which have at least t common keys, i.e., by (10), they are $j_1 \dots j_t$th associates of each other, for some $j_1 \dots j_t \in \Delta$. Then by Lemma 4.1, the set $\Omega = \{i : 1 \le i \le t,\ j_i = 0 \ \text{ or } \ 2\}$ is nonempty. For $i \in \Omega$, let $\delta_{j_i}(i)$ equal 1 or r_i according as $j_i = 0$ or 2, respectively. Consider now any nonempty subset Γ of Ω. Then for $i \in \Gamma$, as noted in (9), $proj(A, i)$ and $proj(A', i)$ are identical if $j_i = 0$, while $proj(A, i)$ and $proj(A', i)$ have exactly one common key if $j_i = 2$. Define $H(A, A'; \Gamma)$ as the collection of nodes A'', such that for every $i \in \Gamma$, $proj(A'', i)$ is different from $proj(A, i)[= proj(A', i)]$ whenever $j_i = 0$, and $proj(A'', i)$ does not include the single key common to $proj(A, i)$ and $proj(A', i)$ whenever $j_i = 2$.

Lemma 5.1 *With reference to any two distinct nodes A and A' which are $j_1 \dots j_t$th associates of each other, where $j_1 \dots j_t \in \Delta$, the cardinality of $H(A, A'; \Gamma)$ defined as above is given by*

$$\sigma(\Gamma) = \left(\prod_{i \in \Gamma}\{b_i - \delta_{j_i}(i)\}\right)\left(\prod_{i \notin \Gamma} b_i\right).$$

Proof of Lemma 5.1 In view of the definition of the $\delta_{j_i}(i)$, this is evident from (4) on recalling that every symbol occurs in r_i blocks of d_i by condition (II) of Subsection 2.2. □

Theorem 5.1 *Let* $\xi_{j_1 \ldots j_t} = \Pi_{i=1}^{t} \xi_{j_i}(i)$, *where*

$$\xi_0(i) = 1 - (1 - b_i^{-1})^s, \;\; \xi_1(i) = 1, \;\; \xi_2(i) = 1 - (1 - r_i b_i^{-1})^s, \;\; 1 \leq i \leq t.$$

Then for $s < \min(k_1, \ldots, k_t)$,

$$\text{fail}(s) \approx 1 - \left(\frac{n}{n-2}\right)^s + \left(\frac{n}{n-2}\right)^s \frac{\sum_{\Delta} n_{j_1 \ldots j_t} \xi_{j_1 \ldots j_t}}{\sum_{\Delta} n_{j_1 \ldots j_t}}.$$

Proof of Theorem 5.1 Consider two distinct nodes A and A'. Let D denote the event that they have at least $q(= t)$ common keys and F denote the event that the link between them fails when out of the remaining $n-2$ nodes, s randomly chosen ones are compromised. Then

$$\text{fail}(s) = P(F|D) = P(F \cap D)/P(D). \tag{24}$$

As in the proof of Theorem 4.1, let $E(j_1 \ldots j_t)$ denote the event that A and A' are $j_1 \ldots j_t$th associates of each other. Then by (10) and (15),

$$P(D) = \sum_{\Delta} P\{E(j_1 \ldots j_t)\} = \frac{\sum_{\Delta} n_{j_1 \ldots j_t}}{n-1}. \tag{25}$$

Similarly,

$$\begin{aligned} P(F \cap D) &= \sum_{\Delta} P\{F \cap E(j_1 \ldots j_t)\} \\ &= \sum_{\Delta} P\{E(j_1 \ldots j_t)\} P\{F|E(j_1 \ldots j_t)\} \\ &= \sum_{\Delta} \frac{n_{j_1 \ldots j_t}}{n-1} P\{F|E(j_1 \ldots j_t)\}. \end{aligned} \tag{26}$$

In order to find an expression for the conditional probability in (26), take any fixed $j_1 \ldots j_t \in \Delta$, and condition on the event that A and A' are $j_1 \ldots j_t$th associates of each other. Then as noted in the context of Lemma 5.1, the set $\Omega = \{i : 1 \leq i \leq t, j_i = 0 \text{ or } 2\}$ is nonempty. By (9), $proj(A, i)$ and $proj(A', i)$ have one or more common keys *if and only if* $i \in \Omega$. For any such i, let G_i denote the event that not all of the key(s) common to $proj(A, i)$ and $proj(A', i)$ occur in one or more of the s randomly chosen nodes that are compromised. Then for the fixed $j_1 \ldots j_t$ under consideration, by the usual union intersection formula,

$$P\{F|E(j_1 \ldots j_t)\} = 1 - P\{\cup_{i \in \Omega} G_i\} = 1 + \sum_{\Gamma \subseteq \Omega} (-1)^{|\Gamma|} P(\cap_{i \in \Gamma} G_i), \tag{27}$$

where the sum on the extreme right is over all nonempty subsets Γ of Ω, and $|\Gamma|$ denotes the cardinality of Γ. Note that the right side of (27) depends on $j_1 \dots j_t$ through Ω.

For any fixed nonempty subset Γ of Ω, we now find the probability $P(\cap_{i\in\Gamma} G_i)$ appearing in (27). Denote the s randomly chosen nodes that are compromised by $A_1^*, \dots, A_s^*$. Fix any $i \in \Gamma$, so that $j_i = 0$ or 2. First suppose $j_i = 0$. Then $proj(A, i)$ and $proj(A', i)$ are identical, and G_i happens *if and only if*, for each $1 \le l \le s$, $proj(A_l^*, i)$ is different from $proj(A, i)[= proj(A', i)]$. The *only if* part of this claim is obvious. The *if* part follows because any two distinct blocks of d_i intersect in at most one symbol or key (*vide* condition (IV) of Subsection 2.2) and $s < \min(k_1, \dots, k_t)$. Next, let $j_i = 2$. Then $proj(A, i)$ and $proj(A', i)$ have exactly one common key and G_i happens *if and only if*, for each $1 \le l \le s$, $proj(A_l^*, i)$ does not include this single common key. Recalling the definition of $H(A, A'; \Gamma)$, it is now clear that $\cap_{i\in\Gamma} G_i$ happens *if and only if* each of $A_1^*, \dots, A_s^*$ belongs to $H(A, A'; \Gamma)$. So, as $n = \prod_{i=1}^t b_i$, by Lemma 5.1, we get

$$\begin{aligned} P(\cap_{i\in\Gamma} G_i) &= \frac{\binom{\sigma(\Gamma)}{s}}{\binom{n-2}{s}} \approx \left(\frac{\sigma(\Gamma)}{n-2}\right)^s \\ &= \left(\frac{n}{n-2}\right)^s \left(\frac{\sigma(\Gamma)}{n}\right)^s \\ &= \left(\frac{n}{n-2}\right)^s \prod_{i\in\Gamma} \left(1 - \frac{\delta_{j_i}(i)}{b_i}\right)^s. \end{aligned} \tag{28}$$

Since $\xi_{j_i}(i) = 1$ for $j_i = 1$, i.e., for $i \notin \Omega$, and

$$1 - \left(1 - \frac{\delta_{j_i}(i)}{b_i}\right)^s = \xi_{j_i}(i),$$

for $j_i = 0$ or 2, i.e., for $i \in \Omega$, substitution of (28) in (27) yields

$$\begin{aligned} P\{F|E(j_1 \dots j_t)\} &\approx 1 + \left(\frac{n}{n-2}\right)^s \sum_{\Gamma\subseteq\Omega} (-1)^{|\Gamma|} \prod_{i\in\Gamma} \left(1 - \frac{\delta_{j_i}(i)}{b_i}\right)^s \\ &= 1 - \left(\frac{n}{n-2}\right)^s + \left(\frac{n}{n-2}\right)^s \prod_{i\in\Omega} \left[1 - \left(1 - \frac{\delta_{j_i}(i)}{b_i}\right)^s\right] \\ &= 1 - \left(\frac{n}{n-2}\right)^s + \left(\frac{n}{n-2}\right)^s \prod_{i=1}^t \xi_{j_i}(i) \\ &= 1 - \left(\frac{n}{n-2}\right)^s + \left(\frac{n}{n-2}\right)^s \xi_{j_1 \dots j_t}. \end{aligned} \tag{29}$$

If we now substitute (29) in (26) and then substitute (25) and (26) in (24) the result follows. □

Remark 5.1 The approximation in (28) and hence that in Theorem 5.1 is in the spirit of Lee and Stinson (2008). It is quite accurate when n and $\sigma(\Gamma)$ are large and s is relatively small, which is typically the case. □

Remark 5.2 The condition $s < \min(k_1, \ldots, k_t)$ in Theorem 5.1 is not severe because typically s is not large. Moreover, it can be checked that for the case $q = t = 1$, Theorem 5.1 remains valid even without this condition. □

Examples 4.1 and 4.3 are now revisited with a view to illustrating Theorem 5.1. Example 4.4 can also be treated in the same way as Example 4.3 and so is not shown here.

Example 5.1 Example 4.1 (continued). Here $t = 1$, $n = b_1$ and, irrespective of whether d_1^* is a PBIB design with $\lambda_1 = 0,\ \lambda_2 = 1$, or a BIB design with $\lambda = 1$, we have $\Delta = \{2\}$. Hence Theorem 5.1 yields

$$\text{fail}(s) \approx 1 - \left(\frac{n}{n-2}\right)^s + \left(\frac{n}{n-2}\right)^s \xi_2(1) = 1 - \left(\frac{b_1 - r_1}{b_1 - 2}\right)^s. \tag{30}$$

□

Remark 5.3 As a continuation of Remarks 3.1 and 4.3, we now see that the fail(s) values of the linear scheme constructed in Lee and Stinson (2008) also follow from Thoerem 5.1. Since their scheme has $b_1 = p^2$ and $r_1 = p$, on substituting these in our expression (30) we get

$$\text{fail}(s) \approx 1 - \left(\frac{p^2 - p}{p^2 - 2}\right)^s.$$

This matches the expression for fail(s) in their Subsection 4.1.1. □

Example 5.2 Example 4.3 (continued). Here $t = 2$, $\theta_1(1) > 0$, $\theta_1(2) = 0$, $n = b_1 b_2$ and $\Delta = \{02, 10, 20, 22\}$. As noted earlier,

$$n_{02} = \theta_2(2),\ n_{10} = \theta_1(1),\ n_{20} = \theta_2(1), n_{22} = \theta_2(1)\theta_2(2). \tag{31}$$

Also,

$$\begin{aligned}
\xi_{02} &= \{1 - (1 - b_1^{-1})^s\}\{1 - (1 - r_2 b_2^{-1})^s\}, \\
\xi_{10} &= 1 - (1 - b_2^{-1})^s, \\
\xi_{20} &= \{1 - (1 - r_1 b_1^{-1})^s\}\{1 - (1 - b_2^{-1})^s\}, \\
\xi_{22} &= \{1 - (1 - r_1 b_1^{-1})^s\}\{1 - (1 - r_2 b_2^{-1})^s\}.
\end{aligned} \tag{32}$$

One can now readily apply Theorem 5.1 to find fail(s). □

6 Applications

As mentioned earlier, our method of construction, based on (4) and applicable to any $q(\geq 1)$, can yield KPSs for widely diverse values of the underlying parameters such as the number of nodes n, the number of keys per node k and the key pool size v, thus enabling the practitioner to find a suitable KPS depending on the requirements of a given situation. This flexibility arises because of the freedom in choosing the PBIB or BIB designs $d_1^*, \ldots, d_t^*$ that one starts with while applying (4). Furthermore, the analytical results in the last two sections can be applied to ensure that the resulting KPSs behave nicely with regard to local connectivity and resiliency, as measured by Pr and fail(s).

In order to give a flavor of the points noted above without making the presentation too long, we now focus on the case $q = 2$ and in the next three subsections present three applications where d_1^* is a PBIB design based on the (a) GD, (b) triangular and (c) Latin square type association schemes, and d_2^* is a BIB design; note that these correspond to the setup of Example 4.3. The parameter values of the resulting KPSs, obtained via (a), (b) and (c) are seen to be

(a) $n = af(2g+1)$, $k = (a-1)f+g$, $v = \binom{a}{2}f^2 + \frac{1}{3}(2g+1)g$, where $a, f(\geq 2)$ are any integers and $g(\geq 3)$ satisfies $g = 0$ or $1 \pmod 3$,

(b) $n = \binom{m}{2}(2g+1)$, $k = \binom{m-2}{2} + g$, $v = 3\binom{m}{4} + \frac{1}{3}(2g+1)g$, where $m(\geq 4)$ is any integer and g is as in (a),

(c) $n = p^2(2g+1)$, $k = \tilde{k} + g$, $v = \tilde{k}p + \frac{1}{3}(2g+1)g$, where $p(\geq 3)$ and $\tilde{k}(< p+1)$ are integers such that $\tilde{k} - 2$ mutually orthogonal Latin squares of order p exist, and g is as in (a).

Thus these three applications alone are capable of producing KPSs for a wide range of parameter values. Moreover, Theorems 4.1 and 5.1 allow us to explore the properties of these KPSs and the examples in the next three subsections show that they can behave quite well with respect to Pr and fail(s). Indeed, our construction in (4), coupled with these theorems, can easily allow numerous other choices of d_1^* and d_2^* as well, and hence paves the way for obtaining KPSs with an even more versatile range of parameter values, while ensuring attractive values for Pr and fail(s). In contrast, the existing methods of construction are almost invariably design specific, i.e., they employ only BIB designs or only transversal designs and so on, and as a result, it is very difficult for these methods to achieve parameter values as diverse as what is achieved, for instance, in (a)-(c) above. In addition, the existing methods are not always informative about the properties of the resulting KPSs with regard to local connectivity or resiliency. We will

return to this comparison in more detail in the concluding section.

6.1 Use of a PBIB design based on the group divisible association scheme and a BIB design

Suppose the design d_1^* in Example 4.3 is a PBIB design based on the group divisible association scheme as in Example 2.6, with $v_1^* = af,\ b_1^* = \binom{a}{2}f^2, k_1^* = 2,\ r_1^* = (a-1)f,\ \lambda_1 = 0,\ \lambda_2 = 1$. As seen there, such a d_1^* exists for all integers $a, f(\geq 2)$. Also, let the d_2^* in Example 4.3 be a BIB design with $v_2^* = 2g+1,\ b_2^* = \frac{1}{3}(2g+1)g, k_2^* = 3,\ r_2^* = g,\ \lambda = 1$. Such a BIB design corresponds to the Steiner's triple system and it is well known (cf. Kirkman (1847)) that it exists for every integer $g(\geq 3)$ satisfying $g = 0$ or 1 (mod 3). Note that the BIB design in Example 2.1 belongs to this class with $g = 4$.

In our construction (4), now take $t = 2$, with d_1 and d_2 chosen as the dual designs of d_1^* and d_2^*, respectively. Then recalling Definition 2.2, the parameters of d_1 are

$$\begin{gathered} v_1 = \tbinom{a}{2}f^2,\ b_1 = af,\ r_1 = 2,\ k_1 = (a-1)f, \\ \theta_1(1) = f-1,\ \ \theta_2(1) = (a-1)f, \phi_{1,2}^1(1) = 0,\ \ \phi_{2,2}^1(1) = (a-1)f, \end{gathered} \tag{33}$$

and the parameters of d_2 are

$$\begin{gathered} v_2 = \tfrac{1}{3}(2g+1)g,\ b_2 = 2g+1,\ r_2 = 3,\ k_2 = g, \\ \theta_1(2) = 0,\ \theta_2(2) = 2g,\ \phi_{2,2}^2(2) = 2g-1. \end{gathered} \tag{34}$$

The KPS obtained from d_1 and d_2 via (4) has $v = v_1 + v_2 = \binom{a}{2}f^2 + \frac{1}{3}(2g+1)g$ keys and $n = b_1 b_2 = af(2g+1)$ nodes, there being $k = k_1 + k_2 = (a-1)f + g$ keys in every node. For this KPS, substitution of (33) and (34) in (22) yields $\mu_{12} = 2 + (a-1)f(2g+1)$ and hence from (21) and (23) we get

$$\begin{aligned} \mathrm{Pr}_1 &= \frac{af + 2g - 1 + 2(a-1)fg}{af(2g+1) - 1}, \\ \mathrm{Pr}_2 &\approx \frac{2(f-1)g}{af(2g+1)-1}\left[1 - \left(1 - \frac{\mu_{12}}{af(2g+1)-2}\right)^{\eta}\right]. \end{aligned}$$

Similarly, substitution of (33) and (34) in (31) and (32) yields

$$\begin{aligned} n_{02} &= 2g,\ n_{10} = f-1,\ n_{20} = (a-1)f,\ n_{22} = 2(a-1)fg, \\ \xi_{02} &= \left\{1 - \left(1 - \frac{1}{af}\right)^s\right\}\left\{1 - \left(1 - \frac{3}{2g+1}\right)^s\right\}, \end{aligned}$$

$$\xi_{10} = 1-\left(1-\frac{1}{2g+1}\right)^s,$$
$$\xi_{20} = \left\{1-\left(1-\frac{2}{af}\right)^s\right\}\left\{1-\left(1-\frac{1}{2g+1}\right)^s\right\},$$
$$\xi_{22} = \left\{1-\left(1-\frac{2}{af}\right)^s\right\}\left\{1-\left(1-\frac{3}{2g+1}\right)^s\right\}.$$

Theorem 5.1 can now be easily used to find fail(s).

On varying the values of $a,\ f$ and g we can get various choices of d_1^* and d_2^*, leading to KPSs for a variety of parameter values. Two illustrative examples follow.

Example 6.1 Let $a = 2,\ f = 21,\ g = 25$. Then for the resulting KPS, we have $v = 866$, $n = 2142$, $k = 46$, while the values of $\Pr_1$, $\Pr_2$, $\Pr = \Pr_1 + \Pr_2$ for various η and the values of fail(s) for various s are as:

η	1	2	3	4	5	10	15	20
$\Pr_1$	0.5329	0.5329	0.5329	0.5329	0.5329	0.5329	0.5329	0.5329
$\Pr_2$	0.2342	0.3510	0.4092	0.4382	0.4527	0.4667	0.4671	0.4671
Pr	0.7671	0.8839	0.9421	0.9711	0.9856	0.9996	1.0000	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0021	0.0089	0.0198	0.0340	0.0510	0.0703	0.1141	0.1624

□

Example 6.2 Let $a = 2,\ f = 23,\ g = 22$. The resulting KPS has $v = 859$, $n = 2070$, $k = 45$ and the values of $\Pr_1$, $\Pr_2$, $\Pr = \Pr_1 + \Pr_2$ and fail(s) are as:

η	1	2	3	4	5	10	15	20
$\Pr_1$	0.5321	0.5321	0.5321	0.5321	0.5321	0.5321	0.5321	0.5321
$\Pr_2$	0.2346	0.3516	0.4099	0.4390	0.4535	0.4675	0.4679	0.4679
Pr	0.7667	0.8837	0.9420	0.9711	0.9856	0.9996	1.0000	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0022	0.0093	0.0206	0.0352	0.0527	0.0724	0.1169	0.1658

□

6.2 Use of a PBIB design based on the triangular association scheme and a BIB design

Now suppose the design d_1^* in Example 4.3 is a triangular PBIB design as constructed in Example 2.7. Thus d_1^* has $v_1^* = \binom{m}{2},\ b_1^* = 3\binom{m}{4},\ k_1^* = 2,\ r_1^* = \binom{m-2}{2},\ \lambda_1 = 0,\ \lambda_2 = 1$, and as seen there, such a d_1^* exists for every integer $m(\geq 4)$. Also, let us continue with d_2^* as the BIB design considered in Subsection 6.1.

In our construction (4), take $t = 2$, with d_1 and d_2 chosen as the dual designs of d_1^* and d_2^*, respectively. Then recalling Definition 2.2, the parameters of d_1 are

$$v_1 = 3\binom{m}{4},\ b_1 = \binom{m}{2},\ r_1 = 2,\ k_1 = \binom{m-2}{2},$$
$$\theta_1(1) = 2(m-2),\ \theta_2(1) = \binom{m-2}{2},\ \phi_{1,2}^1(1) = m-3,\ \phi_{2,2}^1(1) = \binom{m-3}{2}, \tag{35}$$

while the parameters of d_2 are as in (34). The KPS obtained from d_1 and d_2 via (4) has $v = 3\binom{m}{4} + \frac{1}{3}(2g+1)g$ keys and $n = \binom{m}{2}(2g+1)$ nodes, there being $k = \binom{m-2}{2} + g$ keys in every node. For this KPS, substitution of (34) and (35) in (22) yields $\mu_{12} = 2(m-2) + \binom{m-3}{2}(2g+1)$ and hence from (21) and (23)

$$\begin{aligned}
\mathrm{Pr}_1 &= \frac{m(m-1) + 4g - 2 + 2(m-2)(m-3)g}{m(m-1)(2g+1) - 2}, \\
\mathrm{Pr}_2 &\approx \frac{8(m-2)g}{m(m-1)(2g+1) - 2}\left[1 - \left(1 - \frac{2\mu_{12}}{m(m-1)(2g+1) - 4}\right)^{\eta}\right].
\end{aligned}$$

Similarly, substitution of (34) and (35) in (31) and (32) yields

$$\begin{aligned}
n_{02} &= 2g,\ n_{10} = 2(m-2),\ n_{20} = \binom{m-2}{2},\ n_{22} = (m-2)(m-3)g, \\
\xi_{02} &= \left\{1 - \left(1 - \frac{2}{m(m-1)}\right)^s\right\}\left\{1 - \left(1 - \frac{3}{2g+1}\right)^s\right\}, \\
\xi_{10} &= 1 - \left(1 - \frac{1}{2g+1}\right)^s, \\
\xi_{20} &= \left\{1 - \left(1 - \frac{4}{m(m-1)}\right)^s\right\}\left\{1 - \left(1 - \frac{1}{2g+1}\right)^s\right\}, \\
\xi_{22} &= \left\{1 - \left(1 - \frac{4}{m(m-1)}\right)^s\right\}\left\{1 - \left(1 - \frac{3}{2g+1}\right)^s\right\}.
\end{aligned}$$

Theorem 5.1 can now be employed to find fail(s). Again, on varying m and g we can get KPSs for a variety of parameter values. Two illustrative examples follow.

Example 6.3 Let $m = 9$ and $g = 27$. The resulting KPS has $v = 873$, $n = 1980$, $k = 48$ and the values of Pr_1, Pr_2, $\mathrm{Pr} = \mathrm{Pr}_1 + \mathrm{Pr}_2$ and fail(s) are as:

η	1	2	3	4	5	10	15	20
Pr_1	0.6180	0.6180	0.6180	0.6180	0.6180	0.6180	0.6180	0.6180
Pr_2	0.1620	0.2553	0.3091	0.3400	0.3578	0.3805	0.3819	0.3820
Pr	0.7800	0.8733	0.9271	0.9580	0.9758	0.9985	0.9999	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0021	0.0094	0.0210	0.0362	0.0544	0.0750	0.1216	0.1728

□

Example 6.4 Let $m = 8$ and $g = 31$. The resulting KPS has $v = 861$, $n = 1764$, $k = 46$ and the values of $\Pr_1$, $\Pr_2$, $\Pr = \Pr_1 + \Pr_2$ and fail(s) are as:

η	1	2	3	4	5	10	15	20
$\Pr_1$	0.5780	0.5780	0.5780	0.5780	0.5780	0.5780	0.5780	0.5780
$\Pr_2$	0.1538	0.2515	0.3136	0.3531	0.3782	0.4175	0.4215	0.4220
$\Pr$	0.7318	0.8295	0.8916	0.9311	0.9562	0.9955	0.9995	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0023	0.0103	0.0230	0.0396	0.0593	0.0815	0.1312	0.1853

□

6.3 Use of a PBIB design based on the Latin square type association scheme and a BIB design

Now suppose the design d_1^* in Example 4.3 is a PBIB design based on the Latin square type association scheme and having parameters $v_1^* = p^2,\ b_1^* = \tilde{k}p,\ k_1^* = p,\ r_1^* = \tilde{k},\ \lambda_1 = 0,\ \lambda_2 = 1$. Such a design exists when $p(\geq 3)$ and $\tilde{k}(< p+1)$ are such that $\tilde{k} - 2$ mutually orthogonal Latin squares of order p are available, cf. Definition 2.7. Hence following Definition 2.2, its dual design d_1 has parameters

$$v_1 = \tilde{k}p,\ b_1 = p^2,\ r_1 = p,\ k_1 = \tilde{k},\ \ \theta_1(1) = (p-1)(p+1-\tilde{k}),\ \theta_2(1) = \tilde{k}(p-1),$$
$$\phi_{1,2}^1(1) = \tilde{k}(p-\tilde{k}),\ \phi_{2,2}^1(1) = \tilde{k}(\tilde{k}-1). \tag{36}$$

We continue with d_2 as in the last two subsections and (34) continues to hold for d_2. In our construction (4), now take $t = 2$, with d_1 and d_2 chosen as above.

Clearly, the KPS obtained from d_1 and d_2 via (4) has $v = \tilde{k}p + \frac{1}{3}(2g+1)g$ keys and $n = p^2(2g+1)$ nodes, there being $k = \tilde{k} + g$ keys in every node. For this KPS, substitution of (34) and (36) in (22) yields $\mu_{12} = 2 + 2\tilde{k}(p-\tilde{k}) + \tilde{k}(\tilde{k}-1)(2g+1)$ and hence from (21) and (23) we get

$$\begin{aligned} \Pr_1 &= \frac{p^2 + 2g - 1 + 2\tilde{k}(p-1)g}{p^2(2g+1) - 1}, \\ \Pr_2 &\approx \frac{2(p-1)(p+1-\tilde{k})g}{p^2(2g+1)-1}\left[1 - \left(1 - \frac{\mu_{12}}{p^2(2g+1)-2}\right)^{\eta}\right]. \end{aligned}$$

Similarly, substitution of (34) and (36) in (31) and (32) yields

$$n_{02} = 2g,\ n_{10} = (p-1)(p+1-\tilde{k}),\ n_{20} = \tilde{k}(p-1),\ n_{22} = 2\tilde{k}(p-1)g,$$

$$
\begin{aligned}
\xi_{02} &= \left\{1-\left(1-\frac{1}{p^2}\right)^s\right\}\left\{1-\left(1-\frac{3}{2g+1}\right)^s\right\},\\
\xi_{10} &= 1-\left(1-\frac{1}{2g+1}\right)^s,\\
\xi_{20} &= \left\{1-\left(1-\frac{1}{p}\right)^s\right\}\left\{1-\left(1-\frac{1}{2g+1}\right)^s\right\},\\
\xi_{22} &= \left\{1-\left(1-\frac{1}{p}\right)^s\right\}\left\{1-\left(1-\frac{3}{2g+1}\right)^s\right\}.
\end{aligned}
$$

Theorem 5.1 can now be easily used to find fail(s). Again, KPSs for a variety of parameter values can be obtained by varying the values of p, $\tilde{k}$ and g. Two illustrative examples follow.

Example 6.5 Let $p = 17$, $\tilde{k} = 12$, $g = 28$. Then the resulting KPS has $v = 736$, $n = 16473$, $k = 40$ and the values of Pr_1, Pr_2, $\mathrm{Pr} = \mathrm{Pr}_1 + \mathrm{Pr}_2$ and fail(s) are as:

η	1	2	3	4	5	10	15	20
Pr_1	0.6736	0.6736	0.6736	0.6736	0.6736	0.6736	0.6736	0.6736
Pr_2	0.1515	0.2327	0.2762	0.2995	0.3120	0.3258	0.3264	0.3264
Pr	0.8251	0.9063	0.9498	0.9731	0.9856	0.9994	1.0000	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0030	0.0115	0.0244	0.0410	0.0606	0.0826	0.1320	0.1857

□

Example 6.6 Now let $p = 19$, $\tilde{k} = 13$, $g = 28$. Then the resulting KPS has $v = 779$, $n = 20577$, $k = 41$ and the values of Pr_1, Pr_2, $\mathrm{Pr} = \mathrm{Pr}_1 + \mathrm{Pr}_2$ and fail(s) are as:

η	1	2	3	4	5	10	15	20
Pr_1	0.6571	0.6571	0.6571	0.6571	0.6571	0.6571	0.6571	0.6571
Pr_2	0.1508	0.2353	0.2826	0.3091	0.3240	0.3419	0.3428	0.3429
Pr	0.8079	0.8924	0.9397	0.9662	0.9811	0.9990	0.9999	1.0000

s	1	2	3	4	5	6	8	10
fail(s)	0.0028	0.0104	0.0221	0.0372	0.0551	0.0753	0.1209	0.1710

□

7 Shared key discovery

A major advantage of our construction in (4) is that it makes the task of discovering the keys shared by any two nodes of the resulting KPS quite straightforward. This happens because of the following reasons:

(a) Consider any two distinct nodes A and A'. From (4) and Definition 3.1 it is clear that $proj(A, i)$ and $proj(A', i')$ do not have any common symbol whenever $i \neq i'$. Hence, the set

of keys (symbols) common to A and A' equals the union of the sets of symbols common to $proj(A, i)$ and $proj(A', i)$, the union being over all $i, 1 \leq i \leq t$. As a result, in order to discover the keys shared by A and A', it suffices to find the set of symbols common to $proj(A, i)$ and $proj(A', i)$, *separately* for each i, $1 \leq i \leq t$. This is much simpler than comparing the entire sets of keys in A and A'.

(b) Turning now to the identification of the set of symbols common to $proj(A, i)$ and $proj(A', i)$ for any i, from Definition 3.1 we see that this set is nothing but the set of symbols common to two blocks of d_i. Therefore, in view of the duality between d_i and the design d_i^* that we originally started with, this set is simply the set of blocks labels where the corresponding two symbols of d_i^* occur together. Thus identification of this set becomes particularly easy if the symbols and blocks in d_i^* can be properly labeled so as to obtain algebraically a listing of the symbols appearing in each block of d_i^*. Since the d_i^* considered here are PBIB or BIB designs, such labeling is possible under wide generality. For instance, the commonly used cyclic constructions of these designs, based on one or more initial sets, readily allow such labeling. This kind of labeling is also possible for the constructions described in Examples 2.6 and 2.7.

Indeed in construction (4), each d_i^* can potentially be *any* PBIB design with $\lambda_1 = 0, \lambda_2 = 1$ or *any* BIB design with $\lambda = 1$. Because of such diversity, it is unrealistic in the limited space of this paper to attempt to give an account of the labeling of blocks and symbols, mentioned in (b) above, encompassing *all* possibilities for d_i^*, $i = 1, \ldots, t$. For illustration, therefore, we now revisit the setup of Subsection 6.1 in some detail; those of Subsections 6.2 and 6.3 are briefly touched upon later.

Recall that in Subsection 6.1, d_1^* is a group divisible PBIB design constructed as in Example 2.6. Also d_2^* is a BIB design belonging to the Steiner's triple system, and as seen below, it is generated via a cyclic construction. The parameters of these designs are as described in Subsection 6.1. The facts noted below in (A) and (B) for these two designs will be useful.

(A) *Labels for symbols and blocks of* d_1^**:* Denote the af symbols of d_1^* by ordered pairs $\beta\gamma$, where $\beta\gamma$ is the γth symbol of the βth group; $1 \leq \beta \leq a$ and $1 \leq \gamma \leq f$. Then as indicated in Example 2.6, its $\binom{a}{2} f^2$ blocks are $\{\beta\gamma, \tilde{\beta}\delta\}$, and let these be labeled as $\beta\tilde{\beta}\gamma\delta$, say, where $1 \leq \beta < \tilde{\beta} \leq a$ and $\gamma, \delta \in \{1, 2, \ldots, f\}$. Thus, any two distinct symbols $\beta\gamma$ and $\tilde{\beta}\delta$ occur together in some block *if and only if* $\beta \neq \tilde{\beta}$, and if this happens then the unique block where they occur together has label $\beta\tilde{\beta}\gamma\delta$ if $\beta < \tilde{\beta}$ or $\tilde{\beta}\beta\delta\gamma$ if $\tilde{\beta} < \beta$. Let the label for this block be identified as $L_1(\beta\gamma, \tilde{\beta}\delta)$.

Similarly, the $(a-1)f$ blocks where any symbol $\beta\gamma$ occurs have labels (i) $\beta\tilde{\beta}\gamma\delta$, where $\beta < \tilde{\beta} \leq a$ and $\delta \in \{1, 2, \ldots, f\}$, and (ii) $\tilde{\beta}\beta\delta\gamma$ where $1 \leq \tilde{\beta} < \beta$ and $\delta \in \{1, 2, \ldots, f\}$. Let $V_1(\beta\gamma)$ be the collection of these $(a-1)f$ block labels. □

(B) *Labels for symbols and blocks of d_2^*:* Let $g = 1 \bmod 3$ in d_2^*, i.e., $g = 3h+1$ for some integer $h(\geq 1)$. So d_2^* involves $6h+3$ symbols and $(2h+1)(3h+1)$ blocks. Denote these symbols of d_2^* by ζ_u where $\zeta \in \{0, 1, \ldots, 2h\}$, $u = 0, 1, 2$. Then, the blocks of d_2^* can be represented and labeled as

$$\{(y+z)_x,\ (z-y)_x,\ z_{x+1}\} = xyz, \text{ say, and } \{z_0,\ z_1,\ z_2\} = 0z, \text{ say,}$$

where x, y and z range over $\{0, 1, 2\}$, $\{1, \ldots, h\}$ and $\{0, 1, \ldots, 2h\}$, respectively, and the subscript $x+1$ is reduced modulo 3, while $y+z$ and $z-y$ are reduced modulo $2h+1$. There is a unique block where two distinct symbols ζ_u and $\tilde{\zeta}_w$, $(\zeta, u) \neq (\tilde{\zeta}, w)$, occur together and let the label for this block be identified as $L_2(\zeta_u, \tilde{\zeta}_w)$.

Since y ranges over $\{1, \ldots, h\}$, the following are not hard to observe:
(a) Let $u = w$ and $\zeta \neq \tilde{\zeta}$. Then $L_2(\zeta_u, \tilde{\zeta}_u) = uyz$, where $z = (\zeta + \tilde{\zeta})/2 \bmod 2h+1$ and $y = (\zeta - \tilde{\zeta})/2$ or $(\tilde{\zeta} - \zeta)/2 \bmod 2h+1$, depending on whether $(\zeta - \tilde{\zeta})/2 \bmod 2h+1$ belongs to $\{1, \ldots, h\}$ or $\{h+1, \ldots, 2h\}$.
(b) Let $u \neq w$ and $\zeta = \tilde{\zeta}$. Then $L_2(\zeta_u, \zeta_w) = 0\zeta$.
(c) Let $u \neq w$ and $\zeta \neq \tilde{\zeta}$. Then $L_2(\zeta_u, \tilde{\zeta}_w) = xyz$, where $(x, z) = (u, \tilde{\zeta})$ or (w, ζ), depending on whether $w = u+1$ or $u = w+1 \bmod 3$ and $y = \zeta - \tilde{\zeta}$ or $\tilde{\zeta} - \zeta \bmod 2h+1$, depending on whether $\zeta - \tilde{\zeta} \bmod 2h+1$ belongs to $\{1, \ldots, h\}$ or $\{h+1, \ldots, 2h\}$.

Similarly, the $g(= 3h+1)$ blocks where any symbol ζ_u occurs are labeled as (i) uyz, where $y \in \{1, \ldots, h\}$ and $z = \zeta \pm y \bmod 2h+1$, (ii) $(u-1)y\zeta$, where $y \in \{1, \ldots, h\}$ and $u-1$ is reduced mod 3, and (iii) 0ζ. Let $V_2(\zeta_u)$ be the collection of these $3h+1$ block labels. □

Returning to the setup of Subsection 6.1, consider now the KPS constructed as in (4), with $t = 2$ and d_1 and d_2 chosen as the dual designs of d_1^* and d_2^*, respectively, where d_1^* and d_2^* are as detailed in the facts (A) and (B) above. As seen in Subsection 6.1, this KPS has $v = \binom{a}{2}f^2 + \frac{1}{3}(2g+1)g = \binom{a}{2}f^2 + (2h+1)(3h+1)$ keys and $n = af(6h+3)$ nodes. Since d_1 and d_2 are obtained by interchanging the roles of symbols and blocks in d_1^* and d_2^*, respectively, it is clear from (4) that the v keys correspond to the block labels of d_1^* and d_2^*, while the n nodes correspond to ordered pairs whose first member is a symbol of d_1^* and second member is a symbol of d_2^*.

Thus, using the facts in (A) and (B), the v keys can be denoted by $\beta\tilde{\beta}\gamma\delta$, xyz and $0z$, where

$1 \leq \beta < \tilde{\beta} \leq a$ and $\gamma, \delta \in \{1, 2, \ldots, f\}$, while x, y and z range over $\{0, 1, 2\}$, $\{1, \ldots, h\}$ and $\{0, 1, \ldots, 2h\}$, respectively. Similarly, the n nodes can be labeled as $(\beta\gamma, \zeta_u)$, where $1 \leq \beta \leq a$, $1 \leq \gamma \leq f$, and u and ζ range over $\{0, 1, 2\}$ and $\{0, 1, \ldots, 2h\}$, respectively. Then clearly, the keys appearing in any node $(\beta\gamma, \zeta_u)$ are given by the labels of the blocks of d_1^* containing the symbol $\beta\gamma$ and the labels of the blocks of d_2^* containing the symbol ζ_u. Hence, as discussed in the beginning of this section, the keys shared by two distinct nodes $(\beta\gamma, \zeta_u)$, and $(\tilde{\beta}\delta, \tilde{\zeta}_w)$ are given by the labels of the blocks of d_1^* containing both $\beta\gamma$ and $\tilde{\beta}\delta$ and the labels of the blocks of d_2^* containing both ζ_u and $\tilde{\zeta}_w$, i.e., using the facts noted in (A) and (B), these shared keys are as described below:

(i) the keys in $V_1(\beta\gamma)$ and key $L_2(\zeta_u, \tilde{\zeta}_w)$, if $\beta\gamma = \tilde{\beta}\delta$ and $(\zeta, u) \neq (\tilde{\zeta}, w)$;

(ii) the keys in $V_2(\zeta_u)$, if $\beta = \tilde{\beta}$, $\gamma \neq \delta$ and $(\zeta, u) = (\tilde{\zeta}, w)$;

(iii) the key $L_1(\beta\gamma, \tilde{\beta}\delta)$ and the keys in $V_2(\zeta_u)$, if $\beta \neq \tilde{\beta}$ and $(\zeta, u) = (\tilde{\zeta}, w)$;

(iv) the key $L_2(\zeta_u, \zeta_w)$ if $\beta = \tilde{\beta}$, $\gamma \neq \delta$, and $(\zeta, u) \neq (\tilde{\zeta}, w)$;

(v) the keys $L_1(\beta\gamma, \tilde{\beta}\delta)$ and $L_2(\zeta_u, \tilde{\zeta}_w)$ if $\beta \neq \tilde{\beta}$ and $(\zeta, u) \neq (\tilde{\zeta}, w)$

Thus the keys shared by any two distinct nodes can be found readily from the node labels. Consider any two nodes A and A' in each other's neighborhood and by our construction as described above, suppose they are assigned labels $(\beta\gamma, \zeta_u)$ and $(\tilde{\beta}\delta, \tilde{\zeta}_w)$, respectively. In the shared-key discovery phase, node A only broadcasts the four values β, γ, ζ and u. Once node A' receives these four values, it simply checks them against the corresponding four values in its own label, decides on one of the five cases in (i)-(v) above and accordingly, it immediately identifies its common keys with A. Thus there is no need to solve any equations nor any complicated computations are involved. Path-key establishment is also similarly straightforward.

For further illustration, we revisit the second example of Subsection 6.1, where $a = 2$, $f = 23$ and $g = 22$. Then, as discussed above, the keys of the resulting KPS can be denoted by $12\gamma\delta$, xyz and $0z$, where $\gamma, \delta \in \{1, 2, \ldots, 23\}$, while x, y and z range over $\{0, 1, 2\}$, $\{1, \ldots, 7\}$ and $\{0, 1, \ldots, 14\}$, respectively. Similarly, the nodes of this KPS can be labeled as $(\beta\gamma, \zeta_u)$ where $\beta = 1$ or 2, $1 \leq \gamma \leq 23$, and u and ζ range over $\{0, 1, 2\}$ and $\{0,\ 1,\ldots,\ 14\}$, respectively. From (i) above, the keys shared, for example, by the nodes $(16, 4_0)$ and $(16, 6_0)$ are 126δ, $1 \leq \delta \leq 23$, which constitute $V_1(16)$, and $L_2(4_0, 6_0) = 015$. Similarly, from (v) above, the nodes $(22, 5_1)$ and $(13, 6_2)$ share the keys $L_1(22, 13) = 1232$ and $L_2(5_1, 6_2) = 116$.

The other applications considered in Section 6 allow equally simple discovery of shared keys. The symbols and blocks of the triangular PBIB design in Subsection 6.2 can be represented along

the lines of (A) above. Also, following Lee and Stinson (2008), the blocks of d_1 in Subsection 6.3 can be so labeled that one can readily identify the common symbol, if any, between two given blocks. Furthermore, if $g = 0 \bmod 3$ for the BIB design d_2^*, then one can represent its symbols and blocks in a manner similar to (B) above. These representations readily yield the counterparts of V_1, V_2, L_1 and L_2 for these designs. As a result, for constructions involving these designs, keys shared by any two distinct nodes can again be found easily from the node labels.

8 Comparison of our method with some existing ones

In this paper, we have given a general method for construction of KPSs using duals $d_1, \ldots, d_t$ of PBIB or BIB designs. The most important features of our method can be summarized as follows:

(i) It is applicable to any prespecified intersection threshold $q \geq 1$.

(ii) It allows the construction of KPSs for a wide spectrum of parameter values, namely, the number of nodes n, the number of keys per node k and the key pool size v, thus enabling the user to find a suitable KPS in a given context.

(iii) It ensures that n is multiplicative in the numbers of blocks of $d_1, \ldots, d_t$ while k is additive in the block sizes of these designs. This allows a large n and, at the same time, keeps k in check.

(iv) It comes along with explicit formulae for the local connectivity and resiliency metrics as given by Pr and fail(s). It also keeps the tasks of shared key discovery and path key establishment simple.

As seen earlier, for instance, in the beginning of Section 6 and in Remarks 4.1, 4.2, because of (i)-(iv) above, our method has several advantages compared to the existing ones. We now indicate these advantages in some more detail.

First note that in contrast to (i), the existing methods based on combinatorial designs are typically meant for specific values of q, such as $q = 1$ in Camtepe and Yener (2004, 2007), Lee and Stinson (2005a), Chakrabarty et al. (2006), Dong et al. (2008), Ruj and Roy (2007) and Ruj et al. (2009), or separately for $q = 1$ and $q = 2$ in Lee and Stinson (2008).

Next, as a consequence of (ii), our method allows us to obtain KPSs for networks where the number of nodes n need not be of any specialized form, such as the forms $p(p-1)/2$ or $p(p-1)$ as in Ruj and Roy (2007), or the forms p^2 (for $q = 1$) or p^3 (for $q = 2$), p a prime/prime power, as in Lee and Stinson (2008). Furthermore, because of (iii) and (iv), this can be achieved with

a control on the number of keys k per node, while assuring good values of the performance metrics. To understand why this is important, let $q = 2$ and suppose we start with a scheme of Lee and Stinson (2008) with n equal to the lowest prime power of the form p^3 that exceeds the target number of nodes. If we then discard the unnecessary node allocations to get the final scheme for use, this final scheme will not preserve the Pr and fail(s) values of the original scheme and hence the properties of the final scheme in this regard can become quite erratic. This is because, these performance metrics of the original scheme depend on the pattern of the keys allocated to the different nodes, this allocation having been done by exploiting the structure of some combinatorial design, and once a large number of the allocated nodes are discarded, the underlying combinatorial structure is disrupted, leading to a scheme with uncertain local connectivity and resiliency properties.

For illustration, suppose it is desired to obtain a KPS with about 16500 nodes. Then our Example 6.5 gives a scheme with 16473 nodes with demonstrated good values of the performance metrics. The closest higher prime power of the form p^3 is $27^3 = 19683$. If we start with the scheme of Lee and Stinson (2008) with allocation for 19683 nodes, we will have to delete the allocation for about (19683-16500=)3183 nodes constituting 16.17% of the original 19683 nodes. After such large scale deletion, the Pr and fail(s) values of the final scheme very much depend on the particular nodes deleted and hence become quite arbitrary. Similarly, if about 20500 nodes are needed, then our Example 6.6 gives a scheme with 20577 nodes and assured properties while the nearest scheme of Lee and Stinson (2008) with $29^3 = 24389$ nodes entails a deletion of about 3889, i.e., 15.95%, of the nodes, leading to unpredictable performance. In either of these situations, the constructions in Ruj and Roy (2007), with $n = p(p-1)/2$ or $p(p-1)$ and $k = 2(p-2)$, can bring n close to the target but at the cost of prohibitively large (i.e., 250 or even larger) values of k. In contrast, the schemes in our Examples 6.5 and 6.6 involve only 40 and 41 keys per node. The additive nature of k in our construction, as mentioned in (iii) above, helps in achieving this.

Finally, as noted in (iv), our method comes along with explicit and readily applicable formulae for $\mathrm{Pr} = \mathrm{Pr}_1 + \mathrm{Pr}_2$ and fail(s), and also keeps the tasks of shared key discovery and path key establishment simple. Not all of these aspects have been explored in many of the existing constructions of KPSs via combinatorial designs, and even when this is done, analytical results on Pr and fail(s) are not always available. For example, Dong et al. (2008) studied only Pr_1 and fail(1) for their scheme. Again, as seen in Remark 4.2, the quantity Pr_2 in the Lee and

Stinson (2008) scheme for $q = 2$ does not admit an explicit expression and its calculation calls for design specific numerical enumeration which can be difficult when the number of nodes is large. Similarly, Ruj and Roy (2007) and Ruj et al. (2009) gave some bounds on the expected number of links that will be broken if a specified number of nodes are compromised in their schemes and reported associated simulation results, but did not study fail(s). Incidentally, their schemes have $\mathrm{Pr}_1 = 1$, a feature shared also by our construction when the initial designs $d_1^*, \ldots, d_t^*$ are all taken as BIB designs with $\lambda = 1$; cf. Example 4.1. However, as argued in Lee and Stinson (2008), a scheme with $\mathrm{Pr}_1 = 1$ will have poor connectivity in the event of node compromise as reflected in large fails(s) values. This is why we have focused on schemes with good values of Pr rather than attempting to have $\mathrm{Pr}_1 = 1$.

To sum up, our method of construction is a broad spectrum one which supplements and improves upon the existing methods from various considerations. It is applicable to any intersection threshold $q \geq 1$ and allows the construction of KPSs for widely diverse parameter values. The fact that it is supported by a detailed study of the performance metrics, including explicit formulae for Pr and fail(s), further enhances the scope of its application.

Acknowledgement

The authors thank two referees for their insightful comments which led to an enhancement of the contents and presentation in this version. The work of AD was supported by the Indian National Science Academy under the Senior Scientist Scheme of the Academy. The work of RM was supported by the J. C. Bose National Fellowship of the Govt. of India and a grant from the Indian Institute of Management Calcutta.

References

Blackburn, S. R., Etzion, T., Martin, K. M., and Paterson, M. B. (2010). Distinct Difference Configurations: Multihop Paths and Key Predistribution in Sensor Networks. IEEE Transactions on Information Theory. **56**, 3961-3972.

Carmen, D., Kruus, P., and Matt, B. (2000). Constraints and approaches for distributed sensor network security. Tech. rep. 00-010, NAI Labs.

Camtepe, S. and Yener, B. (2004). Combinatorial design of key predistribution mechanisms for wireless sensor networks. In *ESORICS 2004 Proceedings*. Lecture Notes in Computer

Science, **3193**, Springer, 293-308.

Camtepe, S. and Yener, B. (2007). Combinatorial design of key predistribution mechanisms for wireless sensor networks. *IEEE/ACM Trans. Network.* **15**, 346-358.

Chakrabarti, D., Maitra, S., and Roy, B. (2006). A key-predistribution scheme for wireless sensor networks: merging blocks in combinatorial design. *International Journal of Information Security*, **5**, 105-114

Chan, H., Perrig, A., and Song, D. (2003). Random key predistribution schemes for sensor networks. In *Proceedings of the 2003 Symposium on Security and Privacy.* IEEE Computer Society, 197-213.

Clatworthy, W. H. (1973). Tables of Two-associate Partially Balanced Designs. Natl. Bur. Standards Appl. Math. Ser. No. 63. Washington D.C.

Dong, J., Pei, D., and Wang, X. (2008). A key predistribution scheme based on 3-designs. In *INSCRYPT 2007.* Lecture Notes in Computer Science, **4990**, 81-92, Springer, Berlin.

Dey, A. Incomplete Block Designs. (2010). Hindustan Book Agency, New Delhi

Du, W., Deng, J., Han, Y., Varshney, P., Katz, J., and Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. *ACM Trans. Inform. Syst. Secur.* 8, 228-258.

Eschenauer, L. and Gligor, V. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security.* ACM Press, 41-47

Kirkman, T. P. (1847). On a problem in combinations. *Cambridge and Dublin Math. J.* **2**, 192-204.

Lee, J. and Stinson, D. (2005a). A combinatorial approach to key predistribution for distributed sensor networks. In *IEEE Wireless Communications and Networking Conference (WCNC'05)* **2**, IEEE Communications Society, 1200-1205

Lee, J. and Stinson, D. (2005b). Deterministic key predistribution schemes for distributed sensor networks. In *SAC 2004 Proceedings.* Lecture Notes in Computer Science, **3357**, Springer, 294-307.

Lee, J. and Stinson, D. (2008). On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Trans. Inform. Syst. Secur.* **11**, Article 5.

Martin, K.. (2009). On the applicability of combinatorial designs to key predistribution for

wireless sensor networks In *Proceedings of the 2nd International Workshop on Coding and Cryptology,* Springer, Berlin.

Martin, K., Blackburn, S.R., Etzion, T., and Paterson, M.B. (2010). Distinct difference configurations: multihop paths and key predistribution in sensor networks. *IEEE Transactions in Information Theory,* **56**,3961-3972.

Martin, K., Stinson, D.R., Paterson, M.B. (2011). Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. A*CM Transactions on Sensor Networks,* **7**, No. 2.

Roman, R., Zhou, J., and Lopez, J. (2005). On the security of wireless sensor network. In *ICCSA 2005 Proceedings.* Lecture Notes in Computer Science, Vol 3482. Springer, 681-690

Ruj, S. and Roy, B. (2007). Key predistribution using partially balanced designs in wireless sensor networks. In *Proceedings of ISPA 2007*, Lecture Notes in Computer Science, **4742**, 431-445.

Ruj, S., Seberry, J., and Roy, B. (2009). Key predistribution schemes using block designs in wireless sensor networks. In *Computational Science and Engineering, 2009.* CSE '09., 873-878. DOI 10.1109/CSE.2009.35

Stinson, D. (2003). Combinatorial Designs: Constructions and Analysis. Springer, Berlin, Germany.

Street, A.P. and Street, D.J. (1987). Combinatorics of Experimental Design. Clarendon Press, Oxford.

Younis, M.F., Ghumman, K., and Eltoweissy, C.V. (2006). Location-aware combinatorial key management scheme for clustered sensor networks. *IEEE Transactions on Parallel and Distributed Systems,* **17**, 865-882